# Bounding the order of the vertex-stabiliser in $3$-valent vertex-transitive and $4$-valent arc-transitive graphs

Primož Potočnik    Pablo Spiga    Gabriel Verret

**Abstract**

The main result of this paper is that, if $\Gamma$ is a connected 4-valent $G$-arc-transitive graph and $v$ is a vertex of $\Gamma$, then either $\Gamma$ is one of a well understood infinite family of graphs, or $|G_v| \leq 2^4 3^6$ or $2|G_v| \log_2(|G_v|/2) \leq |\mathrm{V}\Gamma|$ and that this last bound is tight. As a corollary, we get a similar result for $3$-valent vertex-transitive graphs.

**Keywords.** valency $3$, valency $4$, vertex-transitive, arc-transitive, locally-dihedral

## 1 Introduction

The question "how symmetric is a certain mathematical object?" has a venerable history. In general, this question is rather vague but a natural starting point is to consider the order of the automorphism group of the object. This is especially true in the case of finite objects. Of course, larger objects have the potential to admit much larger automorphism groups hence it may be more fruitful to compare the size of the object with the order of its automorphism group. This is the point of view we adopt in this paper. The objects we consider are finite $3$-valent vertex-transitive and $4$-valent arc-transitive graphs. The main result is a striking dichotomy between a well understood family of exceptional graphs, each having a very large automorphisms group and the rest of the graphs with comparatively small automorphism groups.

P. Potočnik: Institute of Mathematics, Physics, and Mechanics, Jadranska 19, 1000 Ljubljana, Slovenia; e-mail: primoz.potocnik@fmf.uni-lj.si

P. Spiga (corresponding author): School of Mathematics and Statistics, The University of Western Australia, Crawley, WA 6009, Australia; e-mail: spiga@maths.uwa.edu.au

G. Verret: Institute of Mathematics, Physics, and Mechanics, Jadranska 19, 1000 Ljubljana, Slovenia; e-mail: gabriel.verret@fmf.uni-lj.si

*Mathematics Subject Classification (2010):* Primary 20B25; Secondary 05E18

We first fix some terminology and mention some background results. Throughout this paper, all graphs considered will be finite, except in Section 7.2. A graph $\Gamma$ is said to be $G$*-vertex-transitive* if $G$ is a subgroup of $\mathrm{Aut}(\Gamma)$ acting transitively on the vertex-set $\mathrm{V}\Gamma$ of $\Gamma$. Similarly, $\Gamma$ is said to be $G$*-arc-transitive* if $G$ acts transitively on the arcs of $\Gamma$ (that is, on the ordered pairs of adjacent vertices of $\Gamma$). When $G = \mathrm{Aut}(\Gamma)$, the prefix $G$ in the above notation is sometimes omitted.

A celebrated theorem of Tutte [29, 30] shows that, if $\Gamma$ is a connected 3-valent $G$-arc-transitive graph, then the stabiliser of a vertex in $G$ has order at most $48$. It is very natural to try to relax the hypothesis of this remarkable theorem by considering valencies greater than 3. In this vein, it can be deduced from the work of Trofimov [27, 28] and Weiss [32] that, if $p$ is a prime, then there exists a constant $c_p$ depending only on $p$ such that, if $\Gamma$ is a connected $p$-valent $G$-arc-transitive graph, then the stabiliser of a vertex in $G$ has order at most $c_p$, generalising the result of Tutte. The situation is quite different when the valency is not a prime, as the next example will show.

We define a family of 4-valent graphs which we will denote $\mathrm{C}(r,s)$. These were studied in detail by Gardiner, Praeger and Xu [10, 20]. We give a definition which is slightly different, but equivalent to the definition used in [10]. Furthermore, as we will be mainly interested in $4$-valent graphs, we simply denote by $\mathrm{C}(r,s)$ the graphs denoted by $\mathrm{C}(2,r,s)$ in [10]. Let $r$ and $s$ be positive integers with $r \geq 3$ and $1 \leq s \leq r-1$. Let $\mathrm{C}(r,1)$ be the lexicographic product $\mathrm{C}_r[\overline{\mathrm{K}_2}]$ of a cycle of length $r$ and an edgeless graph on $2$ vertices. In other words, $\mathrm{V}(\mathrm{C}(r,1)) = \mathbb{Z}_r \times \mathbb{Z}_2$ with $(u,i)$ being adjacent to $(v,j)$ if and only if $|v-u| = 1$. Further, for $s \geq 2$, let $\mathrm{C}(r,s)$ be the graph with vertices being the $(s-1)$-paths of $\mathrm{C}(r,1)$ containing at most one vertex from $\{(y,0),(y,1)\}$ for each $y \in \mathbb{Z}_r$ and with two such $(s-1)$-paths being adjacent in $\mathrm{C}(r,s)$ if and only if their intersection is an $(s-2)$-path in $\mathrm{C}(r,1)$. Clearly, $\mathrm{C}(r,s)$ is a connected $4$-valent graph with $r2^s$ vertices.

There is an obvious action of the wreath product $H = \mathrm{C}_2 \,\mathrm{wr}\, \mathrm{D}_r$ on $\mathrm{C}_r[\overline{\mathrm{K}_2}] = \mathrm{C}(r,1)$ which induces an arc-transitive action on $\mathrm{C}(r,s)$ for $s \leq r-1$. Note that $|H| = 2r2^r$ and hence the order of the stabiliser of a vertex of $\mathrm{C}(r,s)$ in $H$ is $2^{r-s+1}$, which is unbounded. Moreover, if we fix $s$, then the order of the stabiliser of a vertex of $\mathrm{C}(r,s)$ grows exponentially with $r$ and hence exponentially with the number of vertices of $\mathrm{C}(r,s)$.

It has long been suspected that the graphs $\mathrm{C}(r,s)$ are rather exceptional in this respect. For example, Xu asked whether every $4$-valent $G$-arc-transitive graph with $|G_v| > 2^4 3^6$ is isomorphic to some $\mathrm{C}(r,s)$ (see [37, Problem 17]). The answer is negative, as can be seen with a construction of Gardiner and Praeger.

For each $s \geq 3$, they construct an infinite family of $4$-valent $G$-arc-transitive graphs $\Gamma$ (denoted by $\mathrm{C}^{\pm 1}(3,s,s)$ in [10, Definition 2.2]) with $2^{s+1} = |G_v| \leq |V\Gamma|^{\log_3(2)}$. Another example is constructed by Conder and Walker [3], who construct an infinite family of $4$-valent $G$-arc-transitive non-Cayley graphs $\Gamma$ such that $G \cong \mathrm{Sym}(n)$ for some $n$. While

$|G_v|$ is unbounded in both these examples, it grows rather mildly with $|\mathrm{V}\Gamma|$ compared to the exponential growth exhibited by the graphs $\mathrm{C}(r,s)$. In fact, our main result is that, excluding the graphs $\mathrm{C}(r,s)$, $|G_v|$ is indeed bounded above by a sub-linear function of $|\mathrm{V}\Gamma|$. Before we can state Theorem 2 in its full generality, we need to define the following very important concept.

**Definition 1.** Let $P$ be a permutation group, let $\Gamma$ be a connected $G$-vertex-transitive graph and let $v$ be a vertex of $\Gamma$. We denote by $G_v^{\Gamma(v)}$ the permutation group induced by the stabiliser $G_v$ of the vertex $v \in \mathrm{V}\Gamma$ on the neighbourhood $\Gamma(v)$. If $G_v^{\Gamma(v)}$ is permutation isomorphic to $P$, then we say that $(\Gamma, G)$ is *locally-*$P$.

If $\Gamma$ has valency $k$, then the permutation group $G_v^{\Gamma(v)}$ has degree $k$ and, up to permutation isomorphism, does not depend on the choice of $v$. It is an elementary observation that $G_v^{\Gamma(v)}$ is transitive if and only if $\Gamma$ is $G$-arc-transitive and it is regular if and only if $\Gamma$ is $G$-arc-regular, in which case $|G_v| = k$.

Let $\Gamma$ be a connected 4-valent $G$-arc-transitive graph and let $v \in \mathrm{V}\Gamma$. It follows from the work of Gardiner [8] that, if $G_v^{\Gamma(v)}$ is $2$-transitive, then $|G_v| \leq 2^4 3^6$. Up to permutation isomorphism, there is only one transitive permutation group of degree $4$ that is neither regular nor $2$-transitive, namely $\mathrm{D}_4$, the dihedral group of order $8$ in its action on $4$ points. By the elementary observation above together with the work of Gardiner, we obtain that if $|G_v| > 2^4 3^6$, then $(\Gamma, G)$ is locally-$\mathrm{D}_4$. This shows that the hypothesis of our main result is not restrictive.

**Theorem 2.** *Let* $(\Gamma, G)$ *be locally-*$\mathrm{D}_4$*. Then one of the following holds:*

$(A)$ $\Gamma \cong \mathrm{C}(r,s)$ *for some* $r \geq 3$*,* $1 \leq s \leq \frac{r}{2}$*;*

$(B)$ $(\Gamma, G)$ *is one of the pairs in Table 1 or Table 2;*

$(C)$ $|\mathrm{V}\Gamma| \geq 2|G_v|\log_2(|G_v|/2)$.

*Moreover, if* $(C)$ *holds with equality and* $\Gamma$ *is not as in* $(A)$*, then* $(\Gamma, G)$ *is one of* $(\Gamma_t^+, G_t^+)$ *or* $(\Gamma_t^-, G_t^-)$ *for some* $t \geq 2$*.*

Table 1 and Table 2 as well as the definition of the pairs $(\Gamma_t^+, G_t^+)$ and $(\Gamma_t^-, G_t^-)$ can be found in Section 2. If $(\Gamma, G)$ is one of the pairs in Table 1 or Table 2, then $|G_v| \leq 512 < 2^4 3^6$. Hence, Theorem 2 together with the work of Gardiner has the following corollary.

**Corollary 3.** *Let* $\Gamma$ *be a connected* $4$*-valent* $G$*-arc-transitive graph. Then one of the following holds:*

$(A)$ $\Gamma \cong \mathrm{C}(r,s)$ *for some* $r \geq 3$*,* $1 \leq s \leq \frac{r}{2}$*;*

$(B)$ $|G_v| \leq 2^4 3^6$*;*

$(C)$ $|\mathrm{V}\Gamma| \geq 2|G_v| \log_2(|G_v|/2)$.

*Moreover, if* $(C)$ *holds with equality and* $\Gamma$ *is not as in* $(A)$*, then* $(\Gamma, G)$ *is one of* $(\Gamma_t^+, G_t^+)$ *or* $(\Gamma_t^-, G_t^-)$ *for some* $t \geq 2$*.*

For each locally-$\mathrm{D}_4$ pair $(\Gamma, G)$, there is a natural way to construct a $3$-valent $G$-vertex-transitive graph $\mathrm{SG}(\Gamma)$ with $|\mathrm{V}(\mathrm{SG}(\Gamma))| = 2|\mathrm{V}\Gamma|$. In some appropriate sense, this construction is reversible. More details can be found in Section 7.1, where we prove the following:

**Corollary 4.** *Let* $\Gamma$ *be a connected* $3$*-valent* $G$*-vertex-transitive graph. Then one of the following holds:*

$(A)$ $\Gamma = \mathrm{SG}(\Gamma')$ *where either* $\Gamma'$ *appears in Table 1 or in Table 2 or* $\Gamma' \cong \mathrm{C}(r,s)$ *for some* $r \geq 3$*,* $1 \leq s \leq \frac{r}{2}$*;*

$(B)$ $\Gamma$ *is* $G$*-arc-transitive and* $|G_v| \leq 48$*;*

$(C)$ $|\mathrm{V}\Gamma| \geq 8|G_v| \log_2 |G_v|$.

## 1.1 Structure of the paper and sketch of the proof of Theorem 2

Let $(\Gamma, G)$ be locally-$\mathrm{D}_4$. We prove Theorem 2 by considering the action of a minimal normal subgroup $N$ of $G$ on $\mathrm{V}\Gamma$. The *quotient graph* $\Gamma/N$ is the graph whose vertices are the $N$-orbits on $\mathrm{V}\Gamma$ with two such $N$-orbits $v^N$ and $u^N$ adjacent whenever there is a pair of vertices $v' \in v^N$ and $u' \in u^N$ that are adjacent in $\Gamma$. Observe that $G/N$ acts on $\Gamma/N$ arc-transitively, and that the valency of $\Gamma/N$ is either $0$ (when $N$ is transitive on $\mathrm{V}\Gamma$), $1$ (when $N$ has $2$ orbits on $\mathrm{V}\Gamma$), $2$ (when $\Gamma/N$ is a cycle) or $4$. In the latter case, $G/N$ acts faithfully on $\mathrm{V}\Gamma$ and hence $(\Gamma/N, G/N)$ is locally-$\mathrm{D}_4$ with the vertex-stabiliser $(G/N)_{v^N} = G_vN/N$ in $G/N$ isomorphic to $G_v$. Therefore, this will allow the use of an inductive argument when $\Gamma/N$ has valency $4$.

In Section 3 we study the case when $N$ is abelian. Namely, in Section 3.1, we consider the case when $\Gamma/N$ has valency at most $2$. Next, if $\Gamma/N$ has valency $4$, then by induction we may assume that $\Gamma/N$ is one of the graphs in $(A)$ or $(B)$ of Theorem 2. The case when $\Gamma/N$ is as in $(A)$ is dealt with in Section 3.2. Finally, the case when $\Gamma/N$ is as in $(B)$ requires a few computations which are carried out in the proof of Lemma 7.

In Section 4 we study the case when $N$ is non-abelian. The main ingredient in this section is a result on the order of elementary abelian subgroups in simple groups (Theorem 21). The proof of Theorem 21 is very technical, uses the Classification of Finite Simple Groups and is delayed until Section 6.

The proof of Theorem 2 is in Section 5 and consists in collecting all the preceding partial results.

Section 7 consists of applications of our main result and additional remarks. In Section 7.1, we show that the problem of bounding the order of the vertex-stabiliser of a $3$-valent vertex-transitive graph is equivalent to the problem of bounding it for $4$-valent arc-transitive graphs and prove Corollary 4. Finally, in Section 7.2, we explain how to rephrase our results in a purely group theoretical language and how they can be interpreted as bounds on the indices of some normal subgroups in some infinite groups.

**Remark:** Part of the proof of Theorem 2 relies on the Classification of Finite Simple Groups. Using methods similar to the techniques developed in [18], it is possible to prove (without using the Classification of Finite Simple Groups) the following much weaker version of Theorem 2.

**Theorem 5.** *Let* $(\Gamma, G)$ *be locally-*$\mathrm{D}_4$*. Then either* $|G_v| \leq 2|\mathrm{V}\Gamma|^3$ *or* $\Gamma \cong \mathrm{C}(r,s)$ *for some* $1 \leq s \leq r-1$.

# 2 Exceptions in Theorem 2

In this section, we describe the exceptional graphs in Theorem 2 and we state some preliminary results regarding these families that are needed in the rest of the paper. The graphs $\mathrm{C}(r,s)$ were introduced in Section 1.

## 2.1 The graphs $\Gamma_t^+$ and $\Gamma_t^-$.

In this section, we describe the pairs $(\Gamma_t^+, G_t^+)$ and $(\Gamma_t^-, G_t^-)$ mentioned in Theorem 2 (these are the pairs attaining the bound $|\mathrm{V}\Gamma| = 2|G_v|\log_2(|G_v|/2)$ in part $(C)$ of Theorem 2). These graphs are studied in detail in [19] and what follows is a brief overview of some facts relevant for the topic of this paper. The graphs $\Gamma_t^{\pm}$ are defined as *coset graphs* of certain groups $G_t^{\pm}$. The coset graph $\mathrm{Cos}(G,H,a)$ on a group $G$ relative to a subgroup $H \leq G$ and an element $a \in G$ is defined as the graph with vertex set the set of right cosets $G/H = \{Hg \mid g \in G\}$ and with edge set the set $\{\{Hg, Hag\} \mid g \in G\}$.

Let us start by considering the group $E_t$ with the following presentation

$$\begin{aligned} E_t = \langle x_0, \ldots, x_{2t-1}, z \quad | \quad & x_i^2 = z^2 = [x_i, z] = 1 \text{ for } 0 \leq i \leq 2t-1, \\ & [x_i, x_j] = 1 \text{ for } |i-j| \neq t, \\ & [x_i, x_{t+i}] = z \text{ for } 0 \leq i \leq t-1 \rangle. \end{aligned} \tag{1}$$

We note that $E_t$ is the extraspecial group of order $2^{2t+1}$ of “plus type”, that is, the central product of $t$ dihedral groups $\mathrm{D}_4$.

We define two group extensions (namely $G_t^+$ and $G_t^-$) of $E_t$ by the dihedral group

$$\mathrm{D}_{2t} = \langle a, b \mid a^{2t} = b^2 = 1, a^b = a^{-1} \rangle. \tag{2}$$

In both extensions, the generators $a$ and $b$ of $\mathrm{D}_{2t}$ act upon the generators of $E_t$ according to the rules:

$$\begin{aligned} x_i^a &= x_{i+1} \quad \text{for } 0 \leq i \leq 2t-1, \\ x_i^b &= x_{t-1-i} \quad \text{for } 0 \leq i \leq 2t-1, \end{aligned}$$

where the indices are taken modulo $2t$. To obtain the first extension $G_t^+$, we let $a^{2t} = b^2 = 1$ (resulting in a semidirect product), while for the second extension $G_t^-$ we let $a^{2t} = z$, $b^2 = 1$ (resulting in a non-split extension):

$$G_t^+ = E_t \rtimes \mathrm{D}_{2t}, \qquad G_t^- = E_t.\mathrm{D}_{2t}.$$

Finally, let $H_t^{\pm}$ be the subgroup of $G_t^{\pm}$ generated by the elements $\{x_0, \ldots, x_{t-1}, b\}$ and observe that $H_t^+ \cong H_t^- \cong \mathrm{C}_2^t \rtimes \mathrm{C}_2$. Let

$$\Gamma_t^+ = \mathrm{Cos}(G_t^+, H_t^+, a) \text{ and } \Gamma_t^- = \mathrm{Cos}(G_t^-, H_t^-, a).$$

In Proposition 6, we sum up some properties of $\Gamma_t^{\pm}$ which are proved in [19].

**Proposition 6.** *The pairs* $(\Gamma_t^+, G_t^+)$ *and* $(\Gamma_t^-, G_t^-)$ *are locally-*$\mathrm{D}_4$*. For* $t \geq 3$*, the graphs* $\Gamma_t^+$ *and* $\Gamma_t^-$ *are not isomorphic to the graphs* $\mathrm{C}(r,s)$ *for any* $r$ *and* $s$ *and satisfy* $\mathrm{Aut}(\Gamma_t^{\pm}) = G_t^{\pm}$*. Finally,* $\Gamma_2^+ \cong \mathrm{C}(4,3)$*,* $G_2^+ = \mathrm{Aut}(\Gamma_2^+)$*, and* $|\mathrm{Aut}(\Gamma_2^-) : G_2^-| = 9$*.*

## 2.2 The graphs in Table 1 and Table 2.

Most of the graphs in this section are obtained from standard graph operations applied to small $3$-valent arc-transitive graphs. We use the Foster Census notation [4] to denote $3$-valent arc-transitive graphs. For instance, $F_6$ will denote the complete bipartite graph on $6$ vertices, $F_{10}$ the Petersen graph, $F_{14}$ the Heawood graph, $F_{18}$ the Pappus graph, $F_{30}$ the Tutte-Coxeter graph and $F_{90}$ the unique $3$-valent arc-transitive graph with $90$ vertices. The extensive census of 4-valent edge-transitive graphs of small order in [33] is quite useful in understanding the graphs in this section.

Let $\Gamma$ be a graph. The *bipartite double* of $\Gamma$, denoted $\mathrm{B}(\Gamma)$, is the categorical product $\Gamma \times \mathrm{K}_2$, with vertex set $\mathrm{V}(\Gamma) \times \{0,1\}$ and edges $\{(u,i),(v,1-i)\}$ for each edge $\{u,v\}$ of $\Gamma$. The *line graph* of $\Gamma$, denoted $\mathrm{L}(\Gamma)$, has edges of $\Gamma$ as vertices, with two such edges adjacent in $\mathrm{L}(\Gamma)$ if they are adjacent in $\Gamma$. The *arc graph* of $\Gamma$, denoted $\mathrm{AG}(\Gamma)$, has arcs of $\Gamma$ as vertices, with two such arcs $(u,v)$, $(v,w)$ adjacent in $\mathrm{AG}(\Gamma)$ if $u \neq w$. The $3$-*arc graph* of $\Gamma$ (see [14]), denoted $\mathrm{A}_3\mathrm{G}(\Gamma)$, has arcs of $\Gamma$ as vertices, with two such arcs $(v_1,v_2)$, $(w_1,w_2)$ adjacent in $\mathrm{A}_3\mathrm{G}(\Gamma)$ if $w_1$ is adjacent to $v_1$ in $\Gamma$, $v_1 \neq w_2$ and $v_2 \neq w_1$. The *hill capping* (see [34]) of $\Gamma$, denoted $\mathrm{HC}(\Gamma)$, has four vertices $\{u_0,v_0\}$, $\{u_0,v_1\}$, $\{u_1,v_0\}$, $\{u_1,v_1\}$, for each edge $\{u,v\}$ of $\Gamma$, and each $\{u_i,v_j\}$ is adjacent to

| $\Gamma$ | $\lvert V\Gamma\rvert$ | $\lvert G_v\rvert$ | $G$ |
|---|---|---|---|
| $\mathrm{L}(F_6)$ | 9 | 8 | $\mathrm{C}_3^2 \rtimes \mathrm{D}_4$ |
| $\mathrm{B}(\mathrm{L}(F_6))$ | 18 | 8 | $(\mathrm{C}_3^2 \rtimes \mathrm{C}_2) \rtimes \mathrm{D}_4$ |
| $\mathrm{C}_5 \Box \mathrm{C}_5$ | 25 | 8 | $\mathrm{C}_5^2 \rtimes \mathrm{D}_4$ |
| $\mathrm{L}(F_{18})$ | 27 | 8 | $3_+^3 \rtimes \mathrm{D}_4$ |
| $\mathrm{C}^{\pm 1}(3,3,3)$ | 81 | 16 | $(\mathrm{C}_3^3 \rtimes \mathrm{C}_2) \rtimes \mathrm{Sym}(4)$ |

Table 1: Pairs in part $(B)$ of Theorem 2 with $G$ soluble

each $\{v_j, w_{1-i}\}$, where $u$ and $w$ are distinct neighbors of $v$. Finally, the *squared-arc graph* of $\Gamma$ is denoted $\mathrm{A}^2\mathrm{G}(\Gamma)$: the vertices of $\mathrm{A}^2\mathrm{G}(\Gamma)$ are the ordered pairs $((v_1,v_2),(w_1,w_2))$ with $(v_1,v_2)$ and $(w_1,w_2)$ arcs of $\Gamma$, and the edges of $\mathrm{A}^2\mathrm{G}(\Gamma)$ are the 2-sets of the form $\{((v_1,v_2),(w_1,w_2)),((w_1,w_2),(v_2,v_3))\}$ with $v_1,v_2,v_3$ a 2-arc in $\Gamma$.

Except for $\mathrm{C}_5\Box\mathrm{C}_5$ and $\mathrm{C}^{\pm1}(3,3,3)$, all the graphs in Table 1 and Table 2 are obtained by starting with one of the $3$-valent graphs $F_6$, $F_{10}$, $F_{14}$, $F_{18}$, $F_{30}$ or $F_{90}$ and applying some of the graph operations described above. The graph $\mathrm{C}_5\Box\mathrm{C}_5$ is the the cartesian product of two 5-cycles, while $\mathrm{C}^{\pm1}(3,3,3)$ is one of an infinite family of $4$-valent graphs described in [10, Definition $2.2$]. For convenience, we define only $\mathrm{C}^{\pm1}(3,3,3)$. Take $H = \langle m_1, m_2, m_3, g \mid m_i^3 = [m_i,m_j] = 1, g^3 = m_1m_2m_3, m_1^g = m_2, m_2^g = m_3, m_3^g = m_1\rangle$ and define $\mathrm{C}^{\pm1}(3,3,3) = \mathrm{Cay}(H, \{g, g^{-1}, gm_1, (gm_1)^{-1}\})$.

We note that, for all but three pairs $(\Gamma, G)$ appearing in Table 1 and Table 2, we have $G = \mathrm{Aut}(\Gamma)$ and hence the pair is uniquely determined by $\Gamma$. The three exceptional graphs are $\mathrm{L}(F_{30})$, $\mathrm{B}(\mathrm{L}(F_{30}))$ and $\mathrm{B}(\mathrm{L}(F_{10}))$. If $\Gamma$ is one of $\mathrm{L}(F_{30})$ or $\mathrm{B}(\mathrm{L}(F_{30}))$, then $|\mathrm{Aut}(\Gamma) : G| \leq 2$. Finally, the full automorphism group of $\mathrm{B}(\mathrm{L}(F_{10}))$ is locally 2-transitive (in particular, this graph appears in [17, Table 3] as the graph $A[30,1]$), but it contains a subgroup of index 3 which is locally-$\mathrm{D}_4$.

We will need the following two results about the pairs appearing in Table 1 and Table 2.

**Lemma 7.** *Let* $(\Gamma, G)$ *be a locally-*$\mathrm{D}_4$ *pair. Assume that* $G$ *has an abelian minimal normal subgroup* $N$ *such that* $\Gamma/N$ *is* $4$*-valent and that* $(\Gamma/N, G/N)$ *is one of the pairs in Table 1. Then either* $|\mathrm{V}\Gamma| > 2|G_v|\log_2(|G_v|/2)$, $\Gamma = \mathrm{C}(9,1)$ *or* $(\Gamma, G)$ *is one of the pairs in Table 1.*

*Proof.* As $\Gamma/N$ is $4$-valent, the group $N$ acts semiregularly on $\mathrm{V}\Gamma$, $G/N$ acts faithfully on $\mathrm{V}(\Gamma/N)$, $(\Gamma/N, G/N)$ is locally-$\mathrm{D}_4$, the vertex-stabiliser in $G/N$ is isomorphic to $G_v$ and $|\mathrm{V}\Gamma| = |\mathrm{V}(\Gamma/N)||N|$. We may assume that $|\mathrm{V}(\Gamma/N)||N| \leq 2|G_v|\log_2(|G_v|/2)$. Since $|N| \geq 2$, a direct inspection of the pairs in Table 1 reveals that we must have $\Gamma/N = \mathrm{L}(F_6)$ and hence $9|N| \leq 32$. In particular, we may assume that $|N| \leq 3$. The rest of the proof is computational with the help of `Magma` [2]. If $|N| = 2$, then either $\Gamma = \mathrm{C}(9,1)$ or $\Gamma = \mathrm{B}(\mathrm{L}(F_6))$. If $|N| = 3$, then $\Gamma = \mathrm{L}(F_{18})$. $\Box$

| | $\Gamma$ | $\lvert\mathrm{V}\Gamma\rvert$ | $\lvert G_v\rvert$ | $G$ |
|---|---|---|---|---|
| $(i)$ | $\mathrm{L}(F_{10})$ | 15 | 8 | $\mathrm{Sym}(5)$ |
| $(i)a$ | $\mathrm{AG}(F_{10})$ | 30 | 8 | $\mathrm{Sym}(5)\times\mathrm{Sym}(2)$ |
| $(i)b$ | $\mathrm{L}(\mathrm{B}(F_{10}))$ | 30 | 8 | $\mathrm{Sym}(5)\times\mathrm{Sym}(2)$ |
| $(i)c$ | $\mathrm{B}(\mathrm{L}(F_{10}))$ | 30 | 8 | $\mathrm{Sym}(5)\times\mathrm{Sym}(2)$ |
| $(ii)$ | $\mathrm{L}(F_{14})$ | 21 | 16 | $\mathrm{PGL}(2,7)$ |
| $(ii)a$ | $\mathrm{B}(\mathrm{L}(F_{14}))$ | 42 | 16 | $\mathrm{PGL}(2,7)\times\mathrm{Sym}(2)$ |
| $(ii)b$ | $\mathrm{HC}(F_{14})$ | 84 | 16 | $\mathrm{PSL}(2,7)\rtimes\mathrm{D}_4$ |
| $(iii)$ | $\mathrm{L}(F_{30})$ | 45 | 16 or 32 | $G\trianglelefteq_{1,2}\mathrm{P\Gamma L}(2,9)$, $G\neq\mathrm{Sym}(6)$ |
| $(iii)a$ | $\mathrm{B}(\mathrm{L}(F_{30}))$ | 90 | 16 or 32 | $G\trianglelefteq_{1,2}\mathrm{P\Gamma L}(2,9)\times\mathrm{Sym}(2)$ |
| $(iii)b$ | $\mathrm{A}_3\mathrm{G}(F_{30})$ | 90 | 16 | $\mathrm{P\Gamma L}(2,9)$ |
| $(iii)c$ | $\mathrm{L}(F_{90})$ | 135 | 32 | $3.\mathrm{Alt}(6).(\mathrm{C}_2^2)$ |
| $(iii)d$ | $\mathrm{HC}(F_{30})$ | 180 | 32 | $\mathrm{Sym}(6)\rtimes\mathrm{D}_4$ |
| $(iv)$ | $\mathrm{AG}^2(F_{30})$ | 8100 | 512 | $\mathrm{P\Gamma L}(2,9)\,\mathrm{wr}\,\mathrm{Sym}(2)$ |

Table 2: Pairs in part $(B)$ of Theorem 2 with $G$ not soluble
(The notation $H\trianglelefteq_{1,2}K$ means that $H\trianglelefteq K$ and that $|K:H|=1$ or 2.)

**Lemma 8.** *Let $(\Gamma,G)$ be a locally-$\mathrm{D}_4$ pair. Assume that $G$ has a minimal normal subgroup $N$ such that $\Gamma/N$ is 4-valent and that $(\Gamma/N,G/N)$ is one of the pairs in Table 2. Then either $|\mathrm{V}\Gamma|>2|G_v|\log_2(|G_v|/2)$ or $(\Gamma,G)$ is one of the pairs in Table 2.*

*Proof.* As $\Gamma/N$ is $4$-valent, the group $N$ acts semiregularly on $\mathrm{V}\Gamma$, $G/N$ acts faithfully on $\mathrm{V}(\Gamma/N)$, $(\Gamma/N,G/N)$ is locally-$\mathrm{D}_4$, the vertex-stabiliser in $G/N$ is isomorphic to $G_v$ and $|\mathrm{V}\Gamma|=|\mathrm{V}(\Gamma/N)||N|$. We may assume that $|\mathrm{V}(\Gamma/N)||N|\leq 2|G_v|\log_2(|G_v|/2)$. Since $|N|\geq 2$, a direct inspection of the pairs in Table 2 reveals that we must have that the pair $(\Gamma/N,G/N)$ is either in row $(i)$ with $|N|=2$, in row $(ii)$ with $|N|\leq 4$, in row $(ii)a$ with $|N|=2$, in row $(iii)$ with $|N|\leq 5$ and $|G_v|=32$, or in row $(iii)a$ with $|N|=2$ and $|G_v|=32$.

We use `Magma` to deal with these cases. If $(\Gamma/N,G/N)$ is in row $(i)$, $(ii)$ or $(ii)a$, then $|G|=|G/N||N|<2000$ and hence $G$ must appear in the `SmallGroups` database of `Magma`. For each candidate group $G$, we compute the list of core-free subgroups $Q$ of $G$ of order $|G_vN/N|$ and we construct the permutation representation of $G$ on the right cosets of $Q$ in $G$. Finally, we check whether there exists a self-paired suborbit of size $4$ giving rise to a connected locally-$\mathrm{D}_4$ pair. The only pairs arising in this way are already in Table 2.

We now assume that $(\Gamma/N,G/N)$ is in row $(iii)$ (respectively $(iii)a$) and hence $G/N$ is isomorphic to $\mathrm{P\Gamma L}(2,9)$ (respectively $\mathrm{P\Gamma L}(2,9)\times\mathrm{Sym}(2)$). Consider the socle $S/N=\mathrm{soc}(G/N)$. We have $S/N\cong\mathrm{Alt}(6)$ (respectively $S/N\cong\mathrm{Alt}(6)\times\mathrm{C}_2$) and $S/N$ is transitive on $V(\Gamma/N)$. Therefore $S$ acts transitively on $V\Gamma$ and $|S|=|S/N||N|\leq 2000$. In particular, the group $S$ can be found in the `SmallGroups` database. It can be checked

that the stabiliser of the vertex $v^N$ in $S/N$ has two orbits on $\Gamma(v^N)$ and hence $S_v$ has two orbits on $\Gamma(v)$. For each candidate $S$, we compute the list of core-free subgroups $Q$ of $S$ of order $|S_vN/N|$ and we construct the permutation representation of $S$ on the right cosets of $Q$ in $S$. Finally we check whether there exists two distinct self-paired suborbits of size $2$ whose union gives rise to a connected locally-$\mathrm{D}_4$ pair. The only pairs arising in this way are already in Table 2. □

# 3 $G$ has an abelian minimal normal subgroup $N$

## 3.1 $\Gamma/N$ has valency at most 2

The case when the quotient is a cycle was examined in some details in [10] and we report some results that follow from their work.

**Theorem 9** ([10], Theorem 1.1, Lemma 3.1)**.** *Let $\Gamma$ be a connected $4$-valent $G$-arc-transitive graph and let $N$ be a minimal normal $p$-subgroup of $G$ with orbits of size $p^s$, for some prime $p$. Let $K$ denote the kernel of the action of $G$ on the $N$-orbits. Suppose that the quotient $\Gamma/N$ is a cycle of length $r \geq 3$. Then either $G$ has an abelian normal subgroup that is not semiregular on the vertices of $\Gamma$, or $p$ is odd and $K_v$ is a nontrivial elementary abelian $2$-group of order dividing $2^s$.*

One of the cases in the conclusion of Theorem 9 is that $G$ has an abelian normal subgroup that is not semiregular on the vertices of $\Gamma$. It turns out that this is a very strong restriction, as seen in the following theorem, which is [20, Theorem $1$ with $p = 2$ ].

**Theorem 10.** *Suppose that $\Gamma$ is a connected $4$-valent $G$-arc-transitive graph, and that $G$ has an abelian normal subgroup which is not semiregular on the vertices of $\Gamma$. Then $\Gamma \cong \mathrm{C}(r,s)$ for some $r \geq \max\{3, s+1\}$, $s \geq 1$.*

As noted in the introduction, there is an obvious action of $\mathrm{C}_2^r \rtimes \mathrm{D}_r$ on $\mathrm{C}(r,s)$. It turns out that, when $r \neq 4$, this is in fact the full automorphism group.

**Theorem 11** ([20], Theorem $2.13$)**.** *Let $\Gamma = \mathrm{C}(r,s)$ and let $H = \mathrm{C}_2^r \rtimes \mathrm{D}_r$. If $r \neq 4$, then $\mathrm{Aut}(\Gamma) = H$. Moreover, $|\mathrm{Aut}(\mathrm{C}(4,1)) : H| = 9$, $|\mathrm{Aut}(\mathrm{C}(4,2)) : H| = 3$ and $|\mathrm{Aut}(\mathrm{C}(4,3)) : H| = 2$.*

Combining the two previous theorems, we get the following locally-$\mathrm{D}_4$ version of Theorem 10, which will be used repeatedly.

**Corollary 12.** *Let $(\Gamma, G)$ be a locally-$\mathrm{D}_4$ pair and let $v$ be a vertex of $\Gamma$. If $G$ has an abelian normal subgroup which is not semiregular on the vertices of $\Gamma$, then $\Gamma \cong \mathrm{C}(r,s)$ for some $1 \leq s \leq r-2$. Moreover, if $|\mathrm{V}\Gamma| \leq 2|G_v|\log_2(|G_v|/2)$, then $s \leq \frac{r}{2}$.*

*Proof.* By Theorem 10, we have $\Gamma \cong \mathrm{C}(r,s)$ for some $r \geq \max\{3, s+1\}$, $s \geq 1$. To show the first claim, it suffices to show that $r \neq s+1$. Suppose, on the contrary, that $r = s+1$. If $r \neq 4$, then it follows from Theorem 11 that $|\mathrm{Aut}(\mathrm{C}(r,r-1))_v| = |\mathrm{C}_2^r \rtimes \mathrm{D}_r|/|\mathrm{V}(\mathrm{C}(r,r-1))| = 2^{r+1}r/(2^{r-1}r) = 4$ and hence $(\Gamma, G)$ cannot be locally-$\mathrm{D}_4$, which is a contradiction. If $r = 4$, then $s = 3$. By Theorem 11, $|\mathrm{Aut}(\mathrm{C}(4,3))_v| = 8$ and hence $G = \mathrm{Aut}(\mathrm{C}(4,3))$. It can be checked that every abelian normal subgroup of $\mathrm{Aut}(\mathrm{C}(4,3))$ acts semiregularly on the vertices of $\mathrm{C}(4,3)$, which contradicts the hypothesis of Corollary 12.

We now assume that $|\mathrm{V}\Gamma| \leq 2|G_v|\log_2(|G_v|/2)$ and show that $s \leq \frac{r}{2}$. From the first part of the proof, we have $1 \leq s \leq r-2$ and hence we may assume that $r > 4$. Suppose, on the contrary, that $s > \frac{r}{2}$ and hence $r-s \leq s-1$. It follows from Theorem 11 that $|G_v| \leq |\mathrm{Aut}(\Gamma)_v| = |\mathrm{C}_2^r \rtimes \mathrm{D}_r|/|\mathrm{V}\Gamma| = r2^{r+1}/(r2^s) = 2^{r-s+1}$ and hence $2|G_v|\log_2(|G_v|/2) \leq (r-s)2^{r-s+2}$. If $r-s = s-1$, then $2|G_v|\log_2(|G_v|/2) \leq (s-1)2^{s+1} < (2s-1)2^s = r2^s = |\mathrm{V}\Gamma|$, which is a contradiction. Hence, we may assume that $r-s \leq s-2$ and hence $2|G_v|\log_2(|G_v|/2) \leq (r-s)2^s < r2^s = |\mathrm{V}\Gamma|$, which is also a contradiction. □

The main result of this section is the following.

**Theorem 13.** *Let $(\Gamma, G)$ be a locally-$\mathrm{D}_4$ pair. Assume that $G$ has an abelian minimal normal subgroup $N$ such that $\Gamma/N$ has valency at most 2. Then one of the following holds:*

$(A)$ $\Gamma \cong \mathrm{C}(r,s)$ *for some* $r \geq 3$, $1 \leq s \leq \frac{r}{2}$*;*

$(B)$ $(\Gamma, G)$ *is one of the pairs in Table 1 with* $\Gamma \neq \mathrm{L}(F_{18})$*;*

$(C)$ $|\mathrm{V}\Gamma| > 2|G_v|\log_2(|G_v|/2)$.

*Proof.* If $G$ has an abelian normal subgroup that is not semiregular on $\mathrm{V}\Gamma$, then, by Corollary 12, part $(A)$ or $(C)$ holds. We will therefore assume that every abelian normal subgroup of $G$ acts semiregularly on $\mathrm{V}\Gamma$. Write $|N| = p^s$, for some prime $p$ and $s \geq 1$.

Suppose first that $\Gamma/N$ is a cycle of length $r \geq 3$. Let $K$ denote the kernel of the action of $G$ on the $N$-orbits. Since $\Gamma/N$ is a cycle and $(\Gamma, G)$ is locally-$\mathrm{D}_4$, we have $|G_v| = 2|K_v|$. By Theorem 9, we obtain $|\mathrm{V}\Gamma| = rp^s$, $p \geq 3$ and $|K_v|$ divides $2^s$. In particular, $|G_v| \leq 2^{s+1}$ and $s \geq 2$. If $|\mathrm{V}\Gamma| > 2|G_v|\log_2(|G_v|/2)$, then part $(C)$ holds, hence we may assume that $rp^s \leq 2|G_v|\log_2(|G_v|/2) \leq s2^{s+2}$. A simple examination of the cases reveals that we must have $p = r = 3$, $s \in \{2,3,4\}$ and $|G_v| = 2^{s+1}$. In particular, $|K_v| = 2^s$. The graphs for which the equality $|K_v| = 2^s$ is satisfied are classified in [10, Theorem 1.1 $(b)$] and a direct inspection of these graphs gives $s = 3$, $\Gamma = \mathrm{C}^{\pm 1}(3,3,3)$ and part $(B)$ follows.

Assume now that $\Gamma/N \cong \mathrm{K}_1$ or $\mathrm{K}_2$. This case was considered already by Gardiner and Praeger [9]. To avoid a tedious consideration of all the cases appearing in their classification, we give an independent argument. If $p = 2$, then (as $G_v$ is a 2-group) $G$ is a 2-group. By minimality of $N$, we get $|N| = 2$, and hence $|\mathrm{V}\Gamma| \le 4$, which is a contradiction. Assume now that $p$ is odd. We show that in this case the kernel $K(v)$ of the action of $G_v$ on $\Gamma(v)$ is trivial, that is, $G_v$ acts faithfully on $\Gamma(v)$. Since $N$ is semiregular, $N$ has precisely 4 orbits on the arcs of $\Gamma$ if $\Gamma/N \cong \mathrm{K}_1$ (respectively, $N$ has precisely 4 orbits on the edges of $\Gamma$ if $\Gamma/N \cong \mathrm{K}_2$). Note that $K(v)$ fixes each of these $N$-orbits setwise. On the other hand, for each vertex $u$, every element of a vertex-stabiliser $G_u$ which fixes each of the $N$-orbits on arcs (respectively, edges) setwise is in $K(u)$. By connectivity of $\Gamma$, this implies that $K(v)$ fixes every vertex of $\Gamma$, and hence is trivial. In particular, this shows that $G_v \cong \mathrm{D}_4$. If $|\mathrm{V}\Gamma| > 32$, then part $(C)$ holds. We shall therefore assume that $|\mathrm{V}\Gamma| \le 32$.

Consider the action of $G_v$ on $N$ by conjugation. If this action is not faithful, then a nontrivial element $x$ of $G_v$ centralising $N$ fixes every vertex in the $N$-orbit $v^N$. In particular, $N$ has two orbits on $\mathrm{V}\Gamma$ forming a bipartition of $\Gamma$. Since $x \neq 1$, this implies that $u^x \neq u$ for a neighbour $u$ of $v$, and in particular, $u$ and $u^x$ share the same neighbourhood. It is then easy to show that $\Gamma \cong \mathrm{C}(r, 1)$ for some $r \ge 3$ (see [16, Lemma 4.3]), and part $(A)$ follows.

We may therefore assume that $G_v$ acts faithfully on $N$ by conjugation, that is, $\mathrm{Aut}(N)$ contains a subgroup isomorphic to $G_v \cong \mathrm{D}_4$. In particular, since the automorphism group of a group of prime order is cyclic, we have $s \ge 2$. If $\Gamma/N \cong \mathrm{K}_2$, then $32 \ge |\mathrm{V}\Gamma| = 2p^s$, and hence $p = 3$ and $s = 2$. It easy to see that $\Gamma \cong \mathrm{B}(\mathrm{L}(F_6))$ from which part $(B)$ follows. On the other hand, if $\Gamma/N \cong \mathrm{K}_1$, then $N$ acts regularly on $\mathrm{V}\Gamma$ and therefore $\Gamma = \mathrm{Cay}(N, S)$ for some inverse-closed generating subset $S$ of $N$. In particular, since $|S| = 4$, $N$ is generated by 2 elements, and hence $s = 2$. Moreover, since $32 \ge |\mathrm{V}\Gamma| = p^2$, it follows that $p \in \{3, 5\}$. It is then easy to see that $\Gamma = \mathrm{L}(F_6)$ or $\mathrm{C}_5 \square \mathrm{C}_5$ from which part $(B)$ follows. $\square$

## 3.2 $\Gamma/N \cong \mathrm{C}(r, s)$

In this section we deal with the case where the quotient $\Gamma/N$ by the abelian minimal normal subgroup $N$ of $G$ is isomorphic to $\mathrm{C}(r, s)$ for some $r \ge 3$, $1 \le s \le \frac{r}{2}$. We first need the following lemma, which is a kind of converse to Corollary 12.

**Lemma 14.** *Let $(\Gamma, G)$ be a locally-$\mathrm{D}_4$ pair. If $\Gamma \cong \mathrm{C}(r, s)$ for some $1 \le s \le r - 2$, then $G$ has an elementary abelian normal 2-subgroup $A$ such that $A$ is not semiregular on $\mathrm{V}\Gamma$, $\Gamma/A$ is a cycle of length $m$ for some multiple $m$ of $r$, $G/A \cong \mathrm{D}_m$ and $A$ is equal to the normal closure $A_v^G$ of $A_v$ in $G$ (where $v \in \mathrm{V}\Gamma$).*

*Proof.* As noted in the introduction, there is an obvious action of $H = B \rtimes \mathrm{D}_r$ with $B = \mathrm{C}_2^r$ on $\Gamma$. Note that $\Gamma/B$ is a cycle of length $r$. Suppose that $r \neq 4$. Then, it follows from Theorem 11 that $H = \mathrm{Aut}(\Gamma)$ and hence $G \leq H$. Moreover $|H_v : B_v| = 2$ and hence $|G \cap H_v : G \cap B_v| = |G_v : G \cap B_v| \leq 2$. Let $A$ be the normal closure of $G \cap B_v$ in $G$. Note that, as $A \leq B$, the group $A$ is an elementary abelian normal 2-subgroup of $G$. Since $(\Gamma, G)$ is locally-$\mathrm{D}_4$, it follows that $G_v$ is not contained in $B_v$ and hence $|G_v : G \cap B_v| = 2$. Since $G \cap B_v$ is contained in $A_v$, it follows that $|G_v : A_v| = 2$, $G \cap B_v = A_v$ and $A = A_v^G$. Since $|G_v| \geq 8$, we have $|A_v| \geq 4$ and hence $A$ is not semiregular on $\mathrm{V}\Gamma$. In particular, $\Gamma/A$ has valency at most 2. Since $A \leq B$ and $\Gamma/B$ is a cycle of length $r \geq 3$, it follows that $\Gamma/A$ is a cycle of length a multiple $m$ of $r$. Finally, since $G/A$ acts arc-transitively on $\Gamma/A$ and $|G_v : A_v| = 2$, it follows that $G/A$ acts faithfully on $\Gamma/A$ and hence $G/A \cong \mathrm{D}_m$.

Assume now that $r = 4$ and, in particular, $s \in \{1, 2\}$. By Theorem 11, $H$ is a Sylow 2-subgroup of $\mathrm{Aut}(\Gamma)$. Since $(\Gamma, G)$ is locally-$\mathrm{D}_4$ and $|\mathrm{V}\Gamma|$ is a power of 2, the group $G$ is a 2-group and hence $G$ is conjugate to a subgroup of $H$. The rest of the proof is as in the previous paragraph. □

The next two lemmas are simply technical and well-known, but we include a proof for the sake of completeness.

**Lemma 15.** *Let $P = \langle x_0, \ldots, x_n \rangle$ be a $p$-group. If, for some $0 \leq i \leq n-1$ and $g \in P$, we have $x_n = x_i^g$, then $P = \langle x_0, \ldots, x_{n-1} \rangle$.*

*Proof.* We recall that $g$ is called a non-generator of $P$ if, for any subset $X$ of $P$, $P = \langle g, X \rangle$ implies that $P = \langle X \rangle$. In a $p$-group, every commutator is a non-generator, see [22, 5.3.2]. Assume $x_n = x_i^g$, for some $0 \leq i \leq n-1$ and $g \in P$. We have

$$\begin{aligned} P &= \langle x_0, \ldots, x_{n-1}, x_n \rangle = \langle x_0, \ldots, x_{n-1}, x_i^g \rangle = \langle x_0, \ldots, x_{n-1}, x_i[x_i, g] \rangle \\ &= \langle x_0, \ldots, x_{n-1}, [x_i, g] \rangle = \langle x_0, \ldots, x_{n-1} \rangle. \end{aligned}$$

□

**Lemma 16.** *Let $q$ be an odd prime power and let $H$ be an elementary abelian $2$-subgroup of $\mathrm{GL}(n, q)$ of order $2^r$. Then $H$ is conjugate to a subgroup of the group consisting of the scalar matrices. In particular, $r \leq n$.*

*Proof.* Let $D$ be the subgroup of scalar matrices of $\mathrm{GL}(n, q)$. Consider a vector space $V$ of dimension $n$ over $\mathbb{F}_q$ and write $H = \langle h_1, \ldots, h_r \rangle$. We will show that there exists a decomposition $V = \oplus_{i=1}^k V_k$ such that the action of $H$ on $V_i$ is given by the multiplication by $\pm 1$. Note that this implies that $H$ is conjugate to a subgroup of $D$. The proof is by induction on $r$. When $r = 0$, there is nothing to prove. Suppose that $r \geq 1$ and let

$V_+ = \{v + vh_1 \mid v \in V\}$, $V_- = \{v - vh_1 \mid v \in V\}$ and let $v \in V$. Since $q$ is odd, we have

$$v = \left(\frac{v}{2} + \frac{v}{2}h_1\right) + \left(\frac{v}{2} - \frac{v}{2}h_1\right) \in V_+ + V_-$$

and hence $V = V_+ + V_-$. Using the fact that $h_1^2 = 1$, it is easy to check that $V_+$ is the eigenspace corresponding to the eigenvalue $1$ of $h_1$ and that $V_-$ is the eigenspace corresponding to the eigenvalue $-1$ of $h_1$. Let $v \in V_+$ and $h \in H$. As $H$ is abelian, we have $vh = vh_1h = (vh)h_1$ and hence $vh \in V_+$. This yields that $V_+$ is an $H$-submodule of $V$. Similarly, $V_-$ is an $H$-submodule of $V$. The claim follows by considering the action of $\langle h_2, \ldots, h_r\rangle$ on $V_+$ and on $V_-$ and using the induction hypothesis. Finally, since $D$ is the direct product of $n$ cyclic groups of order $q-1$ and $H$ is conjugate to a subgroup of $D$, we must have $r \leq n$. $\square$

The next theorem is the main result of this section and a key ingredient in the proof of Theorem 2.

**Theorem 17.** *Let $(\Gamma, G)$ be a locally-$\mathrm{D}_4$ pair. Assume that $G$ has an abelian minimal normal $p$-subgroup $N$ such that $\Gamma/N \cong \mathrm{C}(r,s)$ for some $r \geq 3$, $1 \leq s \leq \frac{r}{2}$. Then one of the following holds:*

$(A)$ $\Gamma \cong \mathrm{C}(r', s')$ *for some* $r' \geq 3$, $1 \leq s' \leq \frac{r'}{2}$*;*

$(B)$ $p = 2$ *and* $|\mathrm{V}\Gamma| \geq 2|G_v|\log_2(|G_v|/2)$*;*

$(C)$ $p \geq 3$ *and* $|\mathrm{V}\Gamma| \geq \frac{6}{p}|G_v|^{\log_2(p)}$.

*Moreover, if the inequality in $(B)$ holds with equality and $\Gamma$ is not a graph as in $(A)$, then $(\Gamma, G)$ is one of $(\Gamma_t^+, G_t^+)$ or $(\Gamma_t^-, G_t^-)$ for some $t \geq 2$.*

**Remark:** Note that for $x \geq 8$ and $p \geq 3$, we have $\frac{6}{p}x^{\log_2(p)} > 2x\log_2(x/2)$ and hence if $(C)$ holds, then $|\mathrm{V}\Gamma| > 2|G_v|\log_2(|G_v|/2)$ (the same inequality as in $(B)$).

*Proof.* As $\Gamma/N$ is $4$-valent, we obtain that $N$ is semiregular on $\mathrm{V}\Gamma$. Furthermore, as $\Gamma/N \cong \mathrm{C}(r,s)$ for some $r \geq 3$, $1 \leq s \leq \frac{r}{2}$, it follows that $s \leq r-2$ and hence Lemma 14 implies that $G/N$ contains an elementary abelian normal $2$-subgroup $E/N$ not semiregular on $\mathrm{V}(\Gamma/N)$ with $(\Gamma/N)/(E/N) \cong \Gamma/E$ a cycle of length $m \geq 3$, $(G/N)/(E/N) \cong G/E \cong \mathrm{D}_m$ and $E/N$ is equal to the normal closure $(E_vN/N)^{G/N}$ of $E_vN/N$ in $G/N$. Let $F$ be the normal closure of $E_v$ in $G$. As $N$ is a minimal normal subgroup of $G$, we obtain that either $N \cap F = 1$ or $N \leq F$. If $N \cap F = 1$, then $F \cong FN/N \leq E/N$ is a normal elementary abelian $2$-subgroup of $G$ not acting semiregularly on $\mathrm{V}\Gamma$, and hence by Corollary 12 we obtain that $(A)$ or $(B)$ holds. Therefore we may assume that $N \leq F$. As the normal closure of $E_vN$ in $G$ is $E$, we have $E = (E_vN)^G = E_v^GN = FN = F$, that is, $E = E_v^G$.

Since $\Gamma/E$ is a cycle of length $m \geq 3$ and $G/E \cong \mathrm{D}_m$, it follows that $|G_v| = 2|E_v|$ and $|\mathrm{V}\Gamma| = m|v^E|$ for some vertex $v \in \mathrm{V}\Gamma$. As $E/N$ is an elementary abelian 2-group and $N$ is semiregular, $E_vN/N \cong E_v$ is an elementary abelian 2-group.

Suppose first that $p \geq 3$. Write $|E_v| = 2^t$. Let $C = \mathrm{C}_E(N)$ be the centraliser of $N$ in $E$. Since $N$ and $E$ are normal in $G$, so is $C$. As $(|N|, |C : N|) = 1$, by the Schur-Zassenhaus theorem, $N$ has a complement $K$ in $C$, that is, $C = NK$ and $N \cap K = 1$. Since $K$ centralises $N$, we have $C = N \times K$. It follows that $K$ is characteristic in $C$ and hence normal in $G$. Furthermore as $E/N$ is abelian, the group $K$ is abelian and so is $C$. If $C$ does not act semiregularly on $\mathrm{V}\Gamma$, then $K$ does not act semiregularly on $\mathrm{V}\Gamma$ and, from Corollary 12, we obtain that $(A)$ or $(B)$ holds. Hence we may assume that $C$ acts semiregularly on $\mathrm{V}\Gamma$. In particular, $1 = E_v \cap C = \mathrm{C}_{E_v}(N)$ and the elementary abelian 2-group $E_v$ acts faithfully on $N$ by conjugation. As $|E_v| = 2^t$, Lemma 16 implies $|N| \geq p^t$. Hence

$$|\mathrm{V}\Gamma| = |\mathrm{V}(\Gamma/N)||N| \geq 6|N| \geq 6p^t = \frac{6}{p}(2^{t+1})^{\log_2(p)} = \frac{6}{p}(2|E_v|)^{\log_2(p)} = \frac{6}{p}|G_v|^{\log_2(p)}$$

and part $(C)$ holds.

From now on, we assume that $p = 2$. In particular, $E$ is a 2-group. Fix an orientation of the cycle $\Gamma/E \cong \mathrm{C}_m$, thus obtaining a directed cycle $\vec{\mathrm{C}}_m$. By lifting this orientation to the graph $\Gamma$, we obtain a digraph $\vec{\Gamma}$ of in-degree and out-degree 2, whose underlying graph is $\Gamma$, and such that $\vec{\Gamma}/E \cong \vec{\mathrm{C}}_m$. Observe that the orientation preserving group $G^+ = \mathrm{Aut}(\vec{\Gamma}) \cap G$ has index 2 in $G$, contains the group $E$ and the quotient group $G^+/E$ is cyclic of order $m$.

Let $v$ be a vertex of $\vec{\Gamma}$. Let $t$ be the largest integer such that $E_v$ acts transitively on the $t$-arcs of $\Gamma$ starting at $v$ and let $(v_0, ..., v_t)$, $v_0 = v$, be such a $t$-arc. For $0 \leq i \leq t$, let $E_i$ be the pointwise stabiliser of $\{v_0, ..., v_{t-i}\}$. Consider the action of $E_0$ on the out-neighbours of $v_t$. If this action were transitive, then $E_v$ would act transitively on the $(t+1)$-arcs starting at $v$, contradicting the maximality of $t$. Since $v_t$ has only two out-neighbours, we conclude that $E_0$ must fix them both. Since $\Gamma$ is strongly connected, it follows that $E_0 = 1$ and hence $|E_i| = 2^i$ for $0 \leq i \leq t$. In particular, $|E_t| = |E_v| = 2^t$ and

$$|G_v| = 2|E_v| = 2^{t+1}. \tag{3}$$

As $|G_v| \geq 8$, we have $t \geq 2$. Since $E_v$ is transitive on the $t$-arcs of $\vec{\Gamma}$ starting at $v$ and $G^+$ is vertex-transitive, $G^+$ is transitive on $t$-arcs of $\vec{\Gamma}$. In particular, there exists $a \in G^+$ such that $(v_0, \ldots, v_t)^a = (v_0^a, v_0, \ldots, v_{t-1})$, that is, $v_i = v_0^{a^{-i}}$ for $0 \leq i \leq t$. As $a$ acts as a rotation of order $m$ on $\vec{\Gamma}/E$, we get $G^+ = E\langle a \rangle$. Let $x$ be the generator of the cyclic group $E_1$. For any integer $i$, let $x_i = x^{a^i}$ and $v_i = v_0^{a^{-i}}$ (note that this definition of $v_i$ is consistent with the definition of $v_i$ that we had for $0 \leq i \leq t$).

To make the rest of the proof easier to read, we prove six claims from which the theorem will follow.

CLAIM 1. $E_i = \langle x_0, ..., x_{i-1}\rangle$ for $1 \le i \le t$.

We argue by induction on $i$. If $i = 1$, then by definition, $x = x_0$ and $E_1 = \langle x_0\rangle$. Assume $E_i = \langle x_0, \ldots, x_{i-1}\rangle$ for some $i$ with $1 \le i \le t-1$. As $x$ fixes $\{v_0, \ldots, v_{t-1}\}$ pointwise and $v_t^x \ne v_t$, the element $x_i = x^{a^i}$ fixes $\{v_0^{a^i}, \ldots, v_{t-1}^{a^i}\}$ pointwise and $(v_t^{a^i})^{x_i} \ne v_t^{a^i}$, that is, $x_i$ fixes $\{v_{-i}, \ldots, v_{-i+t-1}\}$ pointwise and $v_{-i+t}^{x_i} \ne v_{-i+t}$. In particular, by definition of $E_{i+1}$, we get $x_i \in E_{i+1} \setminus E_i$. As $|E_{i+1} : E_i| = 2$, we obtain $E_{i+1} = E_i\langle x_i\rangle = \langle x_0, \ldots, x_i\rangle$, completing the induction. ■

For any positive integer $i \ge 1$, we define $E_i = \langle x_0, \ldots, x_{i-1}\rangle$ (Claim 1 shows that, for $1 \le i \le t$, this definition is consistent with the original definition of $E_i$). Note that, for any $i \ge 0$, $E_i \le \langle E_i, E_i^a\rangle = E_{i+1}$. Since $E$ is finite, there exists a smallest $e \ge 0$ such that $E_{t+e} = E_{t+e+1}$. Since $E_{t+e} = E_{t+e+1} = \langle E_{t+e}, E_{t+e}^a\rangle$, it follows that $E_{t+e}$ is normalised by $a$.

CLAIM 2. $E = E_{t+e}$.

Clearly $E_{t+e} \le E$. Moreover, since $\vec{\Gamma}$ is a connected $G^+$-arc-transitive digraph and $a$ maps $v$ to an adjacent vertex, we have that $G^+ = \langle G_v^+, a\rangle = \langle E_t, a\rangle$. It follows that $E_{t+e}$ is normalised by $G^+$. Therefore, as $E_v = E_t$, we obtain $E_{t+e} \ge E_v^{G^+} = \langle E_w \mid w \in \mathrm{V}\Gamma\rangle = E_v^G = E$. ■

From the definition of $e$, we have $|E_{t+i} : E_{t+i-1}| \ge 2$ for $1 \le i \le e$ and hence $|E_{t+e} : E_t| \ge 2^e$. In particular, Claim 2 gives

$$|v^E| = |E : E_v| = |E_{t+e} : E_t| \ge 2^e. \tag{4}$$

CLAIM 3. $m \ge t + e$.

Assume, by contradiction, that $m < t+e$. In particular, $E = E_{t+e} = \langle x_0, \ldots, x_{t+e-m-1}, \ldots, x_{t+e-1}\rangle$. Since $G^+/E$ is a cyclic group of order $m$ and $a \in G^+$, we get $a^m \in E$ but $x_{t+e-1} = x_{t+e-m-1}^{a^m}$ and hence, by Lemma 15, we have $E_{t+e} = \langle x_0, \ldots, x_{t+e-2}\rangle = E_{t+e-1}$, contradicting the minimality of $e$. ■

Let $\mathrm{Z}(E)$ be the centre of $E$. If $\mathrm{Z}(E)$ does not act semiregularly on $\mathrm{V}\Gamma$, then, by Corollary 12, we obtain that $(A)$ or $(B)$ holds. Therefore we may assume that $\mathrm{Z}(E)$ acts semiregularly on $\mathrm{V}\Gamma$. Recall that $E_v = E_t = \langle x_0, \ldots, x_{t-1}\rangle$ is abelian and hence $E_t^{a^{t-1}} = \langle x_{t-1}, \ldots, x_{2t-2}\rangle$ is also abelian. Therefore $x_{t-1}$ is central in $\langle E_t, E_t^{a^{t-1}}\rangle = \langle x_0, \ldots, x_{2t-2}\rangle = E_{2t-1}$. Since $x_{t-1} \in E_v$ and $\mathrm{Z}(E) \cap E_v = 1$, we get $E_{2t-1} < E = E_{t+e}$ and hence $2t-1 < t+e$ from which it follows that $e \ge t$. Assume $e \ge t+1$. From (4) and Claim 3, we have $|\mathrm{V}\Gamma| = m|v^E| \ge (2t+1)2^{t+1}$. From (3), we have $2|G_v|\log_2(|G_v|/2) = 2t2^{t+1}$ and hence $(B)$ holds with the inequality being strict. Therefore, from now on, we may assume that $e = t$ and, in particular,

$$E = E_{2t} = \langle x_0, \ldots, x_{t-1}, x_t, \ldots, x_{2t-1}\rangle = \langle E_v, E_v^{a^t}\rangle. \tag{5}$$

Since $E$ is a 2-group, $\mathrm{Z}(E)$ intersects every normal subgroup of $E$ non-trivially. In particular, $N \cap \mathrm{Z}(E) \neq 1$. Since $N$ is a minimal normal subgroup of $G$ and $\mathrm{Z}(E)$ is normal in $G$, this implies that $N \leq \mathrm{Z}(E)$. Let $y$ be in $\mathrm{Z}(E)E_v^{a^t} \cap E_v$. Then $y = nx$ for some $n \in \mathrm{Z}(E)$ and $x \in E_v^{a^t}$. Let $g$ be in $E_v^{a^t}$. Using the fact that $n$ is central in $E$, that $x$ and $g$ are in $E_v^{a^t}$ and that $E_v^{a^t}$ is abelian, we see that $y = nx$ commutes with $g$. Since $g$ is an arbitrary element of $E_v^{a^t}$, we obtain that $y$ is centralised by $E_v^{a^t}$. As $E_v$ is abelian and $y \in E_v$, the element $y$ is centralised by $E_v$. Hence, by $(5)$, we obtain $y \in \mathrm{Z}(E) \cap E_v = 1$ and therefore $\mathrm{Z}(E)E_v^{a^t} \cap E_v = 1$. It follows that

$$
\begin{aligned}
|\mathrm{Z}(E)E_v^{a^t}E_v| &= \frac{|\mathrm{Z}(E)E_v^{a^t}||E_v|}{|\mathrm{Z}(E)E_v^{a^t} \cap E_v|} = |\mathrm{Z}(E)E_v^{a^t}||E_v| \qquad (6)\\
&= \frac{|\mathrm{Z}(E)||E_v^{a^t}|}{|\mathrm{Z}(E) \cap E_v^{a^t}|}2^t = |\mathrm{Z}(E)||E_v^{a^t}|2^t = |\mathrm{Z}(E)|2^{2t}.
\end{aligned}
$$

In particular, $|E| \geq |\mathrm{Z}(E)|2^{2t} \geq 2^{2t+1}$ and hence

$$
|\mathrm{V}(\Gamma)| = m|v^E| = m|E : E_v| \geq 2t2^{t+1} = 2|G_v|\log_2(|G_v|/2)
$$

and part $(B)$ holds, with equality if and only if $m = 2t$ and $|E| = 2^{2t+1}$. This concludes the proof of the first part of Theorem 17.

For the remainder of this proof, we assume that $(B)$ holds with equality and that $\Gamma$ is not as in $(A)$. As noted above, we must have $m = 2t$ and $|E| = 2^{2t+1}$, from which it follows that $|\mathrm{Z}(E)| = 2$. It remains to show that $(\Gamma, G)$ is one of $(\Gamma_t^+, G_t^+)$ or $(\Gamma_t^-, G_t^-)$. Since $1 \neq N \leq \mathrm{Z}(E)$, we have $N = \mathrm{Z}(E)$. Furthermore, from $(6)$ we obtain

$$
E = \mathrm{Z}(E)E_v^{a^t}E_v. \qquad (7)
$$

As $E/\mathrm{Z}(E)$ is an elementary abelian 2-group and $E$ is non-abelian, we have $E^2 = [E, E] = \mathrm{Z}(E)$. Write $\mathrm{Z}(E) = \langle z \rangle$.

CLAIM 4.

$$
[x_i, x_j] = \begin{cases} 1 & \text{if } |j-i| \leq t-1, \\ z & \text{if } |j-i| = t. \end{cases}
$$

If $0 \leq j - i \leq t-1$, then $x_i$ and $x_j$ are both contained in $E_t^{a^i} = \langle x_i, \ldots, x_{i+t-1}\rangle$ which is abelian and hence they commute. Suppose that $[x_0, x_t] = 1$. It follows that $x_t$ commutes with $E_v = \langle x_0, \ldots, x_{t-1}\rangle$ and with $E_v^{a^t} = \langle x_t, \ldots, x_{2t-1}\rangle$ and hence is central in $E$, which is contradiction. Hence, $[x_0, x_t] \neq 1$ and, for each $i$, $[x_i, x_{i+t}] = [x_0, x_t]^{a^i} \neq 1$. Since $[E, E] = \mathrm{Z}(E)$, it follows that $[x_i, x_{i+t}] = z$. ■

CLAIM 5. Replacing $a$ by an element in the coset $E_v a$ if necessary, we have

$$
x_i^a = x_{i+1} \text{ (for } 0 \leq i \leq 2t-2), \; x_{2t-1}^a = x_0, \text{ and } v^a \text{ is adjacent to } v.
$$

Since $|G^+ : E| = 2t$, we have that $a^{2t} \in E$. It follows that $x_{2t} = x_0^{a^{2t}} = x_0[x_0, a^{2t}] = x_0 z^\varepsilon$ for some $\varepsilon \in \{0, 1\}$. If $\varepsilon = 0$, then there is nothing to prove. We assume that $\varepsilon = 1$ and let $a' = x_{t-1}a$. By Claim $4$, we get that, for $0 \leq i \leq 2t-2$, $x_i$ commutes with $x_{t-1}$ and hence $x_i^{a'} = x_{i+1}$. Moreover $x_{2t-1}^{a'} = (x_{2t-1}z)^a = x_{2t}z^a = (x_0 z)z = x_0$ and hence the claim is proved replacing $a$ by $a'$. ■

From Claim $5$, it follows that, for every $i$, $x_i^{a^{2t}} = x_i$. Since $a^{2t} \in E$, we have

$$a^{2t} \in \mathrm{Z}(E). \tag{8}$$

Moreover, since $x_{i+2t} = x_i^{a^{2t}} = x_i$, from now on the index $i$ of $x_i$ will be taken modulo $2t$. Let $b$ be an element of $G_v \setminus E_v$.

Claim $6$. Replacing $b$ by an element in the coset $bE_v$ if necessary, we have $x_i^b = x_{t-1-i}$ for every $i$.

Since $b$ normalises $E_v$ and $x_{t-1} \in E_v$, we have $x_{t-1}^b = x_0^{\varepsilon_0} \cdots x_{t-1}^{\varepsilon_{t-1}}$ for some $\varepsilon_i \in \{0, 1\}$. As $G/E \cong \mathrm{D}_m$, we get $(a^{1-t})^b = a^{t-1}y$ for some $y \in E$. Hence

$$\begin{aligned} x_0^b &= x_{t-1}^{a^{1-t}b} = x_{t-1}^{ba^{t-1}y} = (x_0^{\varepsilon_0} \cdots x_{t-1}^{\varepsilon_{t-1}})^{a^{t-1}y} = (x_{t-1}^{\varepsilon_0} \cdots x_{2t-2}^{\varepsilon_{t-1}})^y \\ &= x_{t-1}^{\varepsilon_0} \cdots x_{2t-2}^{\varepsilon_{t-1}}[x_{t-1}^{\varepsilon_0} \cdots x_{2t-2}^{\varepsilon_{t-1}}, y] = x_{t-1}^{\varepsilon_0} \cdots x_{2t-2}^{\varepsilon_{t-1}} z^\varepsilon \end{aligned}$$

for some $\varepsilon \in \{0, 1\}$. Since $x_0^b \in E_v = \langle x_0, \ldots, x_{t-1} \rangle$, from the previous equation we obtain $\varepsilon_1 = \cdots = \varepsilon_{t-1} = \varepsilon = 0$ and $\varepsilon_0 = 1$, that is, $x_0^b = x_{t-1}$ and $x_{t-1}^b = x_0$. Fix $i$ in $\{0, \ldots, t-1\}$ and let $y \in E$ with $(a^{1-t+i})^b = a^{t-1-i}y$. We get $x_i^b = x_{t-1}^{a^{1-t+i}b} = x_{t-1}^{ba^{t-1-i}y} = x_0^{a^{t-1-i}y} = x_{t-1-i}^y = x_{t-1-i}z^\varepsilon$ for some $\varepsilon \in \{0, 1\}$. Since $x_{t-1-i}, x_i^b \in E_v$, we have $\varepsilon = 0$ and hence $x_i^b = x_{t-1-i}$. As $G/E \cong \mathrm{D}_{2t}$, we get $(a^t)^b = a^t y$ for some $y \in E$. Using (7), write $y = z^\varepsilon y_1 y_2$ with $\varepsilon \in \{0, 1\}$, $y_1 \in E_v^{a^t}$ and $y_2 \in E_v$. Let $b' = by_2$. As $y_2 \in E_v$, for $i \in \{0, \ldots, t-1\}$, we have $x_i^{b'} = x_{t-i-1}^{y_2} = x_{t-i-1}$. Fix $i$ in $\{0, \ldots, t-1\}$, we obtain $x_{t+i}^{b'} = x_i^{a^t b y_2} = x_i^{ba^t y y_2} = x_{t-1-i}^{a^t z^\varepsilon y_1} = x_{2t-1-i}^{z^\varepsilon y_1} = x_{2t-1-i}$, where in the last equality we used that $y_1, x_{2t-1-i} \in E_v^{a^t}$ and that $E_v^{a^t}$ is abelian. Hence the claim is proved replacing $b$ by $b'$. ■

From Claim $6$, it follows that $b^2$ centralises $E$. Since $b \in G_v \setminus E_v$, $|G_v : E_v| = 2$ and $E_v \cap \mathrm{Z}(E) = 1$, we have

$$b^2 = 1. \tag{9}$$

As $G/E \cong \mathrm{D}_{2t}$, we get $aa^b \in E$. From Claims $5$ and $6$, we have $x_i^{aa^b} = x_{i+1}^{bab} = x_{t-2-i}^{ab} = x_{t-1-i}^b = x_i$. Therefore $aa^b \in \mathrm{Z}(E)$ and $a^b = a^{-1}z^\varepsilon$ for some $\varepsilon \in \{0, 1\}$. Since $G$ is arc-transitive on $\Gamma$ and $v^a$ is adjacent to $v$, there exists $g \in G$ such that $(v, v^a)^g = (v^a, v)$. It follows that $ag \in G_v$ and $ga^{-1} \in G_v$ which yields $ag \in G_v \cap aG_v a$ and hence $G_v \cap aG_v a = (E_v \cup E_v b) \cap aG_v a \neq \emptyset$. Since $a$ acts as a rotation of order $2t \geq 3$ on $\vec{\Gamma}/E$, we have that the elements in $a^{-2}E = a^{-1}Ea^{-1}$ act fixed-point-freely on $\mathrm{V}\Gamma$. Therefore $a^{-1}Ea^{-1}$ intersects $G_v$ trivially and hence $E_v \cap aG_v a = \emptyset$. This gives $E_v b \cap aG_v a \neq \emptyset$.

Let $yb \in E_v b \cap aG_v a$ with $y = x_0^{\varepsilon_0} \cdots x_{t-1}^{\varepsilon_{t-1}} \in E_v$. As $a^b = a^{-1}z^\varepsilon$, we obtain $a^{-1}yba^{-1} = y^a a^{-1}ba^{-1} = y^a bz^\varepsilon \in G_v$. Since $G_v = E_v \cup E_v b$, it follows that

$$y^a z^\varepsilon = x_1^{\varepsilon_0} \cdots x_{t-1}^{\varepsilon_{t-2}} x_t^{\varepsilon_{t-1}} z^\varepsilon \in E_v$$

and hence $x_t^{\varepsilon_{t-1}} z^\varepsilon \in E_v \cap E_v^{a^t}\mathrm{Z}(E)$. Now (7) yields $E_v \cap E_v^{a^t}\mathrm{Z}(E) = 1$ and hence $\varepsilon = 0$. Therefore

$$a^b = a^{-1}. \tag{10}$$

Recalling the definitions of $(\Gamma_t^+, G_t^+)$ and $(\Gamma_t^-, G_t^-)$ from Section 2.1, it follows from Claims 4, 5 and 6 and from (8), (9) and (10) that either $(\Gamma, G) = (\Gamma_t^+, G_t^+)$ (if $a^{2t} = 1$) or $(\Gamma, G) = (\Gamma_t^-, G_t^-)$ (if $a^{2t} = z$). □

# 4 Case where $G$ has a non-abelian minimal normal subgroup

Our main tool in this section is the following observation, which follows from [7, Theorem].

**Lemma 18.** *Let $(\Gamma, G)$ be a locally-$\mathrm{D}_4$ pair and let $v \in \mathrm{V}\Gamma$. Then $G_v$ is a $2$-group and contains a subgroup $P$ of index $2$ and of nilpotency class at most $2$. Moreover, $P$ contains an elementary abelian $2$-subgroup $E$ of order $2^m$ with $|P| \leq 2^{\lfloor 3m/2 \rfloor}$ and, in particular, $|G_v| \leq 2|E|^{3/2}$.*

As Lemma 18 indicates, the order of $G_v$ in a locally-$\mathrm{D}_4$ pair can be bounded from above by a function of the order of a maximal elementary abelian $2$-group of $G_v$. This motivates the introduction of the following definition.

**Definition 19.** The $2$-*rank* $r_G$ of a finite group $G$ is the minimal number of generators of an elementary abelian $2$-subgroup of maximal order of $G$. We denote by $e_G$ the number $2^{r_G}$, that is, $e_G$ is the order of an elementary abelian $2$-subgroup of $G$ of maximal order.

Before proving the main results of this section we need the following lemma on the $2$-rank of a wreath product.

**Lemma 20.** *Let $W = H \,\mathrm{wr}_\Delta\, K$. If $|H|$ is even, then $e_W \leq e_H^{|\Delta|}$.*

*Proof.* Consider $W$ as a permutation group on $\Omega = H \times \Delta$ where $H$ acts on the set $H$ by right multiplication. We identify the system of imprimitivity $\Sigma = \{H \times \{\delta\} \mid \delta \in \Delta\}$ with $\Delta$, where the block $H \times \{\delta\} \in \Sigma$ is identified with $\delta \in \Delta$. In particular, we say that a subgroup of $W$ is transitive on $\Delta$ if it is transitive on $\Sigma$. Note that the kernel of the action of $W$ on $\Delta$ is $B = H^\Delta$.

Let $E$ be an elementary abelian 2-subgroup of $W$ and let $\mathcal{O}_1, \dots, \mathcal{O}_r$ be the orbits of $E$ on $\Delta$. Note that $E \leq (H \operatorname{wr}_{\mathcal{O}_1} K) \times \cdots \times (H \operatorname{wr}_{\mathcal{O}_r} K)$. We argue by induction on $r$. Assume first that $r = 1$ (that is, $E$ acts transitively on $\Delta$). Let $f$ be an element of $E \cap B$. Let $\delta_1, \delta_2 \in \Delta$ and let $e = \sigma g \in E$ with $\delta_1^\sigma = \delta_2$ where $g \in B$, $\sigma \in K$. Since $E$ is abelian, it follows that $f(\delta_2) = f(\delta_1^\sigma) = f^e(\delta_1) = f(\delta_1)$ and hence $f$ is a constant function of $B$. This yields that $E \cap B$ is isomorphic to an elementary abelian subgroup of $H$ and hence $|E \cap B| \leq e_H$. As $E$ is abelian and transitive on $\Delta$, the group $E/(E \cap B)$ acts regularly on $\Delta$ and hence $|E : E \cap B| = |\Delta|$. It follows that $|E| = |E \cap B||E : E \cap B| \leq e_H|\Delta|$. Since $|H|$ is even, we have $e_H \geq 2$ and hence $e_H|\Delta| \leq e_H^{|\Delta|}$. Assume now that $r \geq 2$. Since $E \leq (H \operatorname{wr}_{\mathcal{O}_1} K) \times \cdots \times (H \operatorname{wr}_{\mathcal{O}_r} K)$, using the induction hypothesis, we obtain

$$|E| \leq \prod_{i=1}^{r} |H \operatorname{wr}_{\mathcal{O}_i} K| \leq \prod_{i=1}^{r} e_H^{|\mathcal{O}_i|} = e_H^{\sum_i |\mathcal{O}_i|} = e_H^{|\Delta|},$$

completing the induction and the proof. □

The following technical theorem is the key ingredient in the proof of our main result for this section. The proof depends heavily on the classification of finite simple groups and includes a very long case-by-case analysis, hence we defer it to Section 6.

**Theorem 21.** *Let $T$ be a non-abelian simple group and $l \geq 1$. Write $l = 2^{l_e} l_o$ with $l_o$ odd, $|T| = 2^t o$ with $o$ odd and $e = e_{\mathrm{Aut}(T)}$. Then either $l_o o^l > 6le^{3l/2}\log_2(e)$ or one of the following holds:*

$(i)$ $l \in \{1, 2, 3, 4\}$ *and* $T = \mathrm{Alt}(5)$ *or* $\mathrm{Alt}(6)$*;*

$(ii)$ $l \in \{1, 2, 4\}$ *and* $T = A_1(8)$ *or* $A_2(2)$*;*

$(iii)$ $l \in \{1, 2\}$ *and* $T = A_1(2^f)$ *(with* $f \in \{4, 5, 6\}$*),* $\mathrm{Alt}(8)$, $A_2(4)$, $B_2(4)$, $B_2(3)$ *or* $B_3(2)$*;*

$(iv)$ $l = 1$ *and* $T = A_1(2^f)$ *(with* $f \in \{7, \dots, 12\}$*),* $M_{12}$, $M_{22}$, $\mathrm{Alt}(7)$, $A_1(11)$, $A_1(13)$, $A_1(25)$, $A_4(2)$, $A_5(2)$, $A_2(3)$, $B_2(8)$, $B_2(16)$, $B_2(32)$, $B_3(4)$, $B_4(2)$, $D_4(2)$, ${}^2A_2(3)$, ${}^2A_5(2)$ *or* ${}^2D_4(2)$.

In the rest of this section, we use a few well-known facts about a group $G$ with a unique minimal normal subgroup $N$ (see [6, Section 4.3]). In particular, if $N$ is non-abelian, we have $N \cong T^l$ for some non-abelian simple group $T$ and for some $l \geq 1$, and $G$ acts transitively on the $l$ simple direct summands of $N$ by conjugation. Moreover, as $\mathrm{C}_G(N) = 1$, the group $G$ can be embedded in $\mathrm{Aut}(N) \cong \mathrm{Aut}(T) \operatorname{wr} \mathrm{Sym}(l)$. With some more computations, we get the following corollary to Theorem 21.

**Corollary 22.** *Let $(\Gamma, G)$ be a locally-$\mathrm{D}_4$ pair. Assume that $G$ has a unique minimal normal subgroup $N$ and that $N$ is isomorphic to $T^l$ where $T$ and $l$ are as in $(i)\ldots(iv)$ of the conclusion of Theorem 21. Then either $|\mathrm{V}\Gamma| > 2|G_v|\log_2(|G_v|/2)$ or $(\Gamma, G)$ is one of the pairs in rows $(i)$, $(ii)$, $(iii)$, $(iii)a$, $(iii)b$ or $(iv)$ of Table 2.*

*Proof.* Note that there are only finitely many pairs $T, l$ appearing in $(i)\ldots(iv)$ of the conclusion of Theorem 21. Therefore this corollary can be proved with the help of a computer. Nevertheless some of the computations involved are non-trivial, hence we give some details on how the result is obtained using `Magma`. Assume $|\mathrm{V}\Gamma| \leq 2|G_v|\log_2(|G_v|/2)$. Given $T$ and $l$ as in the statement, the number of groups $G$ with a unique minimal normal subgroup isomorphic to $T^l$ is very limited (as $|\mathrm{Out}(T)|$ is small). Fix such a $G$ and let $S$ be a Sylow $2$-subgroup of $G$. Let $L$ be the set of divisors $n$ of $|S|$ such that $|G|/n \leq 2n\log_2(n/2)$. These are our candidates for $|G_v|$. In most cases (but not always), $L$ is either the empty set or the set containing only $|S|$. In particular, the number of subgroups $Q$ of $S$ such that $|G : Q| \leq 2|Q|\log_2(|Q|/2)$ is always very small. These are our candidates for $G_v$. For each such $Q$, we check whether $Q$ has a maximal subgroup $P$ of nilpotency class at most $2$. If this is not the case, then, by Lemma 18, we can discard $Q$. Finally, for the remaining $Q$'s, we construct the permutation representation of $G$ on the right cosets of $Q$ and check whether there exists a self-paired suborbit of size $4$ giving rise to a connected locally-$\mathrm{D}_4$ pair. □

We are now ready to prove the main result of this section.

**Theorem 23.** *Let $(\Gamma, G)$ be a locally-$\mathrm{D}_4$ pair. Assume that $G$ has a non-abelian minimal normal subgroup. Then either $|\mathrm{V}\Gamma| > 2|G_v|\log_2(|G_v|/2)$ or $(\Gamma, G)$ is one of the pairs in Table 2.*

*Proof.* Let $(\Gamma, G)$ be a counter-example to Theorem 23, minimal with respect to $|\mathrm{V}\Gamma|$. Let $v$ be a vertex of $\Gamma$ and let $N$ be a non-abelian minimal normal subgroup of $G$. Assume that $G$ has a minimal normal subgroups $M \neq N$. In particular, $NM = N \times M$. Let $K$ be the kernel of the action of $G$ on the vertices of $\Gamma/M$. Suppose that $N \leq K$. Then $v^N \subseteq v^K \subseteq v^M$. Let $n \in N$ be a non-identity element of odd order. We have $v^n \in v^M$ and hence $v^n = v^m$ for some $m \in M$. This gives $nm^{-1} \in G_v$. Since $|nm^{-1}| = |n||m|$ is not a power of 2 and $G_v$ is a $2$-group, this is a contradiction which yields $N \nleq K$.

By minimality of $N$, we obtain $N \cap K = 1$ and hence the group $N \cong NK/K$ acts faithfully as a group of automorphisms on $\Gamma/M$. Since a connected graph of valency at most $2$ has soluble automorphism group, it follows that $\Gamma/M$ has valency $4$ and hence $K_v = 1$, $K = M$ and $(\Gamma/M, G/M)$ is locally-$\mathrm{D}_4$. By the minimality of $(\Gamma, G)$, we have that either $|\mathrm{V}(\Gamma/M)| > 2|G_v|\log_2(|G_v|/2)$ or $(\Gamma/M, G/M)$ is one of the pairs in Table 2. In the former case, $|\mathrm{V}\Gamma| > |\mathrm{V}(\Gamma/M)|$ and the theorem follows. In the latter case, the theorem follows from Lemma 8.

From now on, we may assume that $N$ is the unique minimal normal subgroup of $G$. Let $T$ be a non-abelian simple group and $l \geq 1$ with $N \cong T^l$. Write $e = e_{\mathrm{Aut}(T)}$, $l = 2^{l_e} l_o$ with $l_o$ odd and $|T| = 2^t o$ with $o$ odd. As $G_v$ is a $2$-group, we have $|\mathrm{V}\Gamma| \geq |G : S|$ where $S$ is a Sylow $2$-subgroup of $G$.

Since $N$ is the unique minimal normal subgroup of $G$, the group $G$ is isomorphic to a subgroup of $\mathrm{Aut}(N) \cong \mathrm{Aut}(T) \,\mathrm{wr}\, \mathrm{Sym}(l)$ and $|G| \geq l|N|$, from which it follows that $|\mathrm{V}\Gamma| \geq |G : S| \geq l_o o^l$. Moreover, by Lemma 20, we have $e_{G_v} \leq e_{\mathrm{Aut}(N)} \leq e^l$. Together with Lemma 18, this yields $|G_v| \leq 2e^{3l/2}$.

If $l_o o^l > 6le^{3l/2}\log_2(e)$, then $|\mathrm{V}\Gamma| \geq l_o o^l > 6le^{3l/2}\log_2(e) = 4e^{3l/2}\log_2(e^{3l/2}) \geq 2|G_v|\log_2(|G_v|/2)$ and the theorem follows. Therefore we may assume that $l_o o^l \leq 6le^{3l/2}\log_2(e)$ and now the conclusion follows from Theorem 21 and Corollary 22. $\square$

# 5 Proof of Theorem 2

*Proof of Theorem 2.* Let $(\Gamma, G)$ be locally-$\mathrm{D}_4$ and $N$ a minimal normal subgroup of $G$. We argue by induction on $|\mathrm{V}\Gamma|$. If $N$ is non-abelian, then from Theorem 23 we get that either part $(B)$ or $(C)$ holds for $(\Gamma, G)$. Furthermore if $(C)$ does hold for $(\Gamma, G)$, then the inequality is strict. Hence we may assume that $N$ is abelian. If $\Gamma/N$ has valency at most $2$, then it follows from Theorem 13 that one of $(A)$, $(B)$ or $(C)$ holds. Furthermore, if $(C)$ does hold, then the inequality is strict. Hence we may assume that $\Gamma/N$ is $4$-valent. In particular, $N$ acts semiregularly on $\mathrm{V}\Gamma$, $(\Gamma/N, G/N)$ is locally-$\mathrm{D}_4$ and the vertex-stabiliser in $G/N$ is isomorphic to $G_v$. By induction, it follows that $(\Gamma/N, G/N)$ satisfies one of $(A)$, $(B)$ or $(C)$.

If $(C)$ holds for $(\Gamma/N, G/N)$, then $|\mathrm{V}\Gamma| = |N||\mathrm{V}(\Gamma/N)| \geq |N|(2|G_v|\log_2(|G_v|/2)) > 2|G_v|\log_2(|G_v|/2)$ and $(C)$ holds for $(\Gamma, G)$ with the inequality being strict. If $(A)$ holds for $(\Gamma/N, G/N)$, then it follows from Theorem 17 (and the subsequent remark) that $(\Gamma, G)$ satisfies $(A)$ or $(C)$. Moreover, if the pair $(\Gamma, G)$ meets the bound in $(C)$ and $\Gamma$ is not as in $(A)$, then $(\Gamma, G) \cong (\Gamma_t^{\pm}, G_t^{\pm})$ for some $t \geq 2$. Suppose now that $(B)$ holds for $(\Gamma/N, G/N)$, that is, $(\Gamma/N, G/N)$ is one of the pairs in Tables 1 and 2. From Lemmas 7 and 8 we obtain that $(B)$ or $(C)$ holds for $(\Gamma, G)$. Furthermore, if $(C)$ does hold, then the inequality is strict. $\square$

# 6 Proof of Theorem 21

We now return to the proof of Theorem 21, which we skipped earlier. The first step is to collect information about the $2$-ranks of non-abelian simple groups, starting with sporadic groups. Table 3 gives $e_T$ when $T$ is a sporadic simple group. This table was obtained using [13] when $T \in \{B, M\}$ and [11, Table $5.6.1$, page $303$] in the rest of the cases.

| $T$ | $M_{11}$ | $M_{12}$ | $M_{22}$ | $M_{23}$ | $M_{24}$ | $J_1$ | $J_2$ | $J_3$ | $J_4$ |
|---|---|---|---|---|---|---|---|---|---|
| $e_T$ | $2^2$ | $2^3$ | $2^4$ | $2^4$ | $2^6$ | $2^3$ | $2^4$ | $2^4$ | $2^{11}$ |
| $T$ | $Co_1$ | $Co_2$ | $Co_3$ | $Suz$ | $Fi_{22}$ | $Fi_{23}$ | $Fi'_{24}$ | $HS$ | $McL$ |
| $e_T$ | $2^{11}$ | $2^{10}$ | $2^4$ | $2^6$ | $2^{10}$ | $2^{11}$ | $2^{11}$ | $2^4$ | $2^4$ |
| $T$ | $He$ | $HN$ | $Th$ | $B$ | $M$ | $O'N$ | $Ly$ | $Ru$ | |
| $e_T$ | $2^6$ | $2^6$ | $2^5$ | $2^{14}$ | $2^{15}$ | $2^3$ | $2^4$ | $2^6$ | |

Table 3: $e_T$ for $T$ a sporadic simple group

The next step is to compute $e_{\mathrm{Alt}(n)}$ and $e_{\mathrm{Sym}(n)}$.

**Lemma 24.** *Let $n$ be a positive integer and write $n = 4m + r$ with $0 \leq r \leq 3$. If $r = 0$ or $1$, then $e_{\mathrm{Sym}(n)} = e_{\mathrm{Alt}(n)} = 2^{2m}$. If $r = 2$ or $3$, then $e_{\mathrm{Sym}(n)} = 2^{2m+1}$ and $e_{\mathrm{Alt}(n)} = 2^{2m}$.*

*Proof.* If $r$ is odd, then a Sylow $2$-subgroup of $\mathrm{Sym}(n)$ fixes some point of $\{1, \ldots, n\}$ and hence is conjugate to a Sylow $2$-subgroup of $\mathrm{Sym}(n-1)$. In particular, we may assume that $r$ is even without loss of generality. Define

$$E_0 = \langle (1,2)(3,4), (1,3)(2,4), \ldots, (m-3, m-2)(m-1, m), (m-3, m-1)(m-2, m)\rangle$$

if $r = 0$, and

$$\begin{aligned} E_0 = {} & \langle (1,2)(3,4), (1,3)(2,4), \ldots, (m-3, m-2)(m-1, m), (m-3, m-1)(m-2, m), \\ & (m+1, m+2)\rangle \end{aligned}$$

if $r = 2$. The group $E_0$ is an elementary abelian $2$-subgroup of $\mathrm{Sym}(n)$ of order $2^{n/2}$ and hence $e_{\mathrm{Sym}(n)} \geq |E_0| = 2^{n/2}$. Let $E$ be an elementary abelian $2$-subgroup of maximal order in $\mathrm{Sym}(n)$ and let $\mathcal{O}_1, \ldots, \mathcal{O}_k$ be the orbits of $E$ on $\{1, \ldots, n\}$. As $E$ is abelian, the action of $E$ on $\mathcal{O}_i$ is regular for every $i$ and hence $|E| \leq \prod_{i=1}^k |\mathcal{O}_i|$. Note that, if $a$ is a power of $2$, then $a \leq 2^{a/2}$ with equality if and only if $a \in \{2, 4\}$. Using the maximality of $|E|$, we have

$$2^{n/2} = |E_0| \leq |E| \leq \prod_{i=1}^{k} |\mathcal{O}_i| \leq \prod_{i=1}^{k} 2^{|\mathcal{O}_i|/2} = 2^{\sum_{i=1}^k |\mathcal{O}_i|/2} = 2^{n/2}.$$

This shows that $e_{\mathrm{Sym}(n)} = 2^{n/2}$. Moreover, this also shows that the order of an elementary abelian $2$-subgroup $E$ of $\mathrm{Sym}(n)$ is $2^{n/2}$ if and only if $E$ is the direct product of the permutation groups induced by $E$ on each of its orbits and each such or bit has size $2$ or $4$.

If $r = 0$, then $E_0 \leq \mathrm{Alt}(n)$ and hence $e_{\mathrm{Alt}(n)} = e_{\mathrm{Sym}(n)}$. Finally, if $r = 2$, then, by the previous paragraph, an elementary abelian subgroup $E$ of $\mathrm{Sym}(n)$ of order $2^{n/2}$ has an orbit of size $2$ and contains a transposition. In particular, $e_{\mathrm{Alt}(n)} < e_{\mathrm{Sym}(n)}$. Since $|E_0 \cap \mathrm{Alt}(n)| = 2^{2m}$, we obtain $e_{\mathrm{Alt}(n)} = 2^{2m}$. $\square$

If $r = 0$, then $E_0 \leq \mathrm{Alt}(n)$ and hence $e_{\mathrm{Alt}(n)} = e_{\mathrm{Sym}(n)}$. Finally, if $r = 2$, then, by the previous paragraph, an elementary abelian subgroup $E$ of $\mathrm{Sym}(n)$ of order $2^{n/2}$ has an orbit of size $2$ and contains a transposition. In particular, $e_{\mathrm{Alt}(n)} < e_{\mathrm{Sym}(n)}$. Since $|E_0 \cap \mathrm{Alt}(n)| = 2^{2m}$, we obtain $e_{\mathrm{Alt}(n)} = 2^{2m}$.

Although there is an extensive literature on the Sylow $2$-subgroups of simple groups of Lie type $T$, we were unable to find an explicit reference for $e_T$ in this case. We wish to thank B. Stellmacher for an enlightening conversation with the second author which inspired the proof of the following technical lemma, where we compute $e_{\mathrm{PSL}(n,q)}$ when $q$ is odd.

**Lemma 25.** *Let $n \geq 1$ and let $q$ be odd. Then $e_{\mathrm{PGL}(n,q)} \leq 2^n$. Also, if $n$ is odd, then $e_{\mathrm{PSL}(n,q)} \leq 2^{n-1}$.*

*Proof.* If $n = 1$, then the result is clear. If $n = 2$, then from the description of the subgroups of $\mathrm{PSL}(2, q)$ in [25, § 6, Theorem 6.25], we obtain $e_{\mathrm{PSL}(2,q)} = 4$ for every odd $q$. Also, as $\mathrm{PGL}(2, q)$ is isomorphic to a subgroup of $\mathrm{PSL}(2, q^2)$ (see [25, § 6, Theorem $6.25$ $(d)$]), we get $e_{\mathrm{PGL}(2,q)} = 4$. Thence, from now on, we may assume $n > 2$.

Let $V$ be an $n$-dimensional vector space over the field with $q$ elements $\mathbb{F}_q$. Write $G = \mathrm{GL}(V)$, $S = \mathrm{SL}(V)$, $\overline{G} = G/\mathrm{Z}(G)$ and $\overline{S} = S/\mathrm{Z}(S)$ where $\mathrm{Z}(G)$ denotes the centre of $G$ and $\mathrm{Z}(S) = S \cap \mathrm{Z}(G)$. Moreover, let $\overline{A}$ be an elementary abelian $2$-subgroup of $\overline{G}$ (respectively $\overline{S}$) and $A$ a $2$-subgroup of $G$ (respectively $S$) such that $\overline{A} = A\mathrm{Z}(G)/\mathrm{Z}(G)$ (respectively $\overline{A} = A\mathrm{Z}(S)/\mathrm{Z}(S)$). We prove two preliminary claims.

CLAIM 1. $|[A, A]| \leq 2$.
Let $a$ and $b$ be in $A$. Since $\overline{A}$ is an elementary abelian $2$-group, we get $a^2 \in \mathrm{Z}(G)$ and $[A, A] \leq \mathrm{Z}(G)$. In particular, as $\mathrm{Z}(G)$ is cyclic, the group $[A, A]$ is cyclic. From one of the basic commutator identities, we obtain $1 = [a^2, b] = [a, b]^a[a, b] = [a, b]^2$. This proves that $[A, A]$ has exponent at most $2$ and therefore $|[A, A]| \leq 2$. ■

Given a subgroup $H$ of $G$ we write $[V, H] = \{v - v^h \mid v \in V, h \in H\}$.

CLAIM 2. Let $a$ and $b$ be in $A$ such that $a^2 = 1$ and $z = [a, b] \neq 1$. We have $[V, \langle a\rangle] = \{v \in V \mid v^a = -v\} = \mathrm{C}_V(az)$ and $[V, \langle az\rangle] = \{v \in V \mid v^{az} = -v\} = \mathrm{C}_V(a)$. Also, $V = [V, \langle a\rangle] \oplus [V, \langle a^b\rangle]$ and $n/2 = \dim_{\mathbb{F}_q}[V, \langle a\rangle]$. In particular, $n$ is even.
By Claim $1$, $z^2 = 1$. Also, as $\overline{A}$ is elementary abelian, $z \in \mathrm{Z}(G)$. Therefore the element $z$ acts on $V$ by the multiplication by $-1$. Let $w$ be in $[V, \langle a\rangle]$, that is, $w = v - v^a$ for some $v \in V$. We have $w^a = (v - v^a)^a = v^a - v^{a^2} = v^a - v = -w$. Conversely, if $w^a = -w$, then $w = w/2 - (w/2)^a \in [V, \langle a\rangle]$. This gives $[V, \langle a\rangle] = \{v \in V \mid v^a = -v\} = \mathrm{C}_V(az)$. Similarly, as $az = a^b$ is conjugate to $a$, we get $[V, \langle az\rangle] = \{v \in V \mid v^{az} = -v\} = \mathrm{C}_V(a)$.

Since the order of $A$ and $V$ are coprime, from [26, § 1, page 7], we have $V = [V, \langle a\rangle] \oplus \mathrm{C}_V(a)$. From the previous paragraph, it follows that $V = [V, \langle a\rangle] \oplus [V, \langle a^b\rangle]$. Finally,

as $\mathrm{C}_V(a)^b = \mathrm{C}_V(a^b) = \mathrm{C}_V(az)$, we get $\dim_{\mathbb{F}_q} \mathrm{C}_V(a) = \dim_{\mathbb{F}_q}[V, \langle a\rangle]$. In particular, $n/2 = \dim_{\mathbb{F}_q}[V, \langle a\rangle]$ and $n$ is even. ■

Assume $A$ is abelian. Since $\overline{A}$ is a quotient of the abelian group $A$, we have $r_{\overline{A}} \leq r_{\Omega_1(A)}$ where $\Omega_1(A) = \{a \in A \mid a^2 = 1\}$. Now, $\Omega_1(A)$ is an elementary abelian 2-subgroup of $G$ (respectively $S$). Hence by Lemma 16, we have $r_{\Omega_1(A)} \leq n$ (respectively $r_{\Omega_1(A)} \leq n-1$) and the bound for $r_{\overline{A}}$ is proved.

Assume $\Omega_1(A) \nleq \mathrm{Z}(A)$ and $A$ is non-abelian. Since not every element of order $2$ of $A$ is contained in the centre of $A$, there exist $a, b \in A$ such that $a^2 = 1$ and $z = [a, b] \neq 1$. By Claim 1, $z$ has order $2$ and $[a, A] = [b, A] = \langle z\rangle$. In particular, $|A : \mathrm{C}_A(a)| = |A : \mathrm{C}_A(b)| = 2$. Writing $B = \mathrm{C}_A(a)$ and $B_1 = B \cap \mathrm{C}_A(b) = \mathrm{C}_A(\langle a, b\rangle)$, we obtain $|A : B_1| = 4$, $|B : B_1| = 2$ and $B = B_1\langle az\rangle$. From Claim 2, we have that $[V, \langle a\rangle] = \{v \in V \mid v^a = -v\}$ and $[V, \langle a\rangle]^b = [V, \langle a^b\rangle] = [V, \langle az\rangle] = \mathrm{C}_V(a)$. Thus, $A$ does not normalise $[V, \langle a\rangle]$. Since $B$ normalises $[V, \langle a\rangle]$ and $|A : B| = 2$, we conclude that $B = N_A([V, \langle a\rangle])$.

Set $C = \mathrm{C}_B([V, \langle a\rangle])$. From Claim 2, we have that $az \in C$ and that

$$C \cap C^b = \mathrm{C}_B([V, \langle a\rangle]) \cap \mathrm{C}_B([V, \langle az\rangle]) = \mathrm{C}_B([V, \langle a\rangle] + [V, \langle az\rangle]) = \mathrm{C}_B(V) = 1.$$

Since $[A, A] = \langle z\rangle$ and $A/\langle z\rangle$ is abelian, the map $x \mapsto [x, b]$ is a group homomorphism from $A$ to $\langle z\rangle$. It follows that $\mathrm{C}_A(b)$ has index 2 in $A$ and hence $\mathrm{C}_C(b)$ has index 2 in $C$ and is contained in $C \cap C^b$. As $C \cap C^b = 1$, we obtain $C = \langle az\rangle$. In particular, $B_1$ acts faithfully on $[V, \langle a\rangle]$.

Set $B_0 = B_1 \cap \mathrm{Z}(\mathrm{GL}([V, \langle a\rangle]))$. We have $A \cap \mathrm{Z}(G) \leq B_0$ and $[B_0, b] = 1$. This shows that $[V, \langle a\rangle]$ and $[V, \langle a\rangle^b]$ are isomorphic $\mathbb{F}_q B_0$-modules. Since $V = [V, \langle a\rangle] \oplus [V, \langle a\rangle^b]$, we get $B_0 \leq \mathrm{Z}(G)$ and $B_0 = A \cap \mathrm{Z}(G)$. Finally, by induction on $\dim_{\mathbb{F}_q} V$, we get

$$|B_1/B_0| = |B_1/(A \cap \mathrm{Z}(G))| \leq 2^{\dim_{\mathbb{F}_q}[V, \langle a\rangle]} = 2^{n/2}.$$

Since $|A : B_1| = 4$, this implies $|\overline{A}| = |A/(A \cap \mathrm{Z}(G))| \leq 4 \cdot 2^{n/2} \leq 2^n$ (where in the last inequality, we used the fact that $n \geq 4$).

Finally, assume that $\Omega_1(A) \leq \mathrm{Z}(A)$ and $A$ is non-abelian. Write $\Omega_1(A) = Z \times A_0$, where $Z = \Omega_1(A) \cap \mathrm{Z}(G)$. Then, by Claim 1, we have that $Z = [A, A]$ and $|Z| = 2$. Recall that $A/(A \cap \mathrm{Z}(G))$ is elementary abelian. Note that, as $A_0 \leq \Omega_1(A) \leq Z(A)$, the group $A_0$ is normal in $A$. If $aA_0$ lies in $A/A_0$ and $aA_0$ has order $2$, then $a^2 \in A_0 \cap \mathrm{Z}(G) = A_0 \cap Z = 1$. This says that the elements of order $2$ in $A/A_0$ are the elements in $\Omega_1(A)/A_0 \cong Z$, that is, $A/A_0$ contains a unique element of order $2$. Thus, $A/A_0$ is the quaternion group of order $8$. In particular, $|\overline{A}| = 4|A_0|$. If $A_0 = 1$, then $|\overline{A}|$ has order $4$ and $4 \leq 2^{n-1}$ (recall that $n \geq 3$). Thus, we may assume that $A_0 \neq 1$. Since the order of $V$ is coprime to $2$, by Lemma 16, the action of the elementary abelian $2$-group $\Omega_1(A)$ on $V$ can be diagonalized. It follows that there exists a subgroup $R$ of index $2$ in $\Omega_1(A)$ such that $\mathrm{C}_V(R) \neq 0$. Since $Z$ acts as the multiplication by $-1$ on $V$, we get $R \cap Z = 1$ and $\Omega_1(A) = Z \times R$.

Therefore, replacing $A_0$ by $R$ if necessary, we may assume that $R = A_0$. By [26, § 1, page 7], we have $V = \mathrm{C}_V(A_0) \times [V, A_0]$. By construction, $\mathrm{C}_V(A_0) \neq 0$, $A_0$ acts faithfully on $[V, A_0]$ and the kernel of the action of $A$ on $\mathrm{C}_V(A_0)$ is $A_0$. It follows by Lemma 16 that $|A_0| \leq 2^r$ (respectively $2^{r-1}$ if $A \leq S$) with $r = \dim_{\mathbb{F}_q}[V, A_0]$. Since $A/A_0 \cong Q_8$ is non-abelian, $s = \dim_{\mathbb{F}_q} \mathrm{C}_V(A_0) \geq 2$. Hence

$$|\overline{A}| = 4|A_0| \leq 2^s \cdot 2^r \leq 2^{r+s} = 2^n \quad (\text{respectively } 2^s \cdot 2^{r-1} = 2^{n-1} \text{ if } A \leq S)$$

and the lemma is proved. □

We now apply Lemma 25 to obtain upper bounds for $e_T$ when $T$ is a simple group of Lie type, which we report in Table 4.

When $T$ has odd characteristic, this bound in obtained by using [12, Table $5.4.C$, page $200$], which lists the minimum degree of a projective representation of every simple group of Lie type, and then applying Lemma 25. For instance, we have that $G_2(q)$ has a projective representation of degree 7, that is, $G_2(q) \leq \mathrm{PSL}(7, q)$. Hence, by Lemma 25, we get $e_{G_2(q)} \leq e_{\mathrm{PSL}(7,q)} = 2^6$. All the entries in the second column of Table 4 are computed with this method.

In the case of groups of even characteristic (except for ${}^2A_2$ and ${}^2B_2$), the bound is obtained by collecting classical and difficult results about the maximal order of unipotent abelian subgroups of $T$. Note that these groups are not necessarily elementary abelian. For example, when $q$ is even, the maximal order of a unipotent abelian subgroup of $E_6(q)$ is $q^{16}$ and a reference for this result is [31]. Therefore $e_{E_6(q)} \leq q^{16}$. We stress that we do not claim that $q^{16} = e_{E_6(q)}$.

Finally, Table 4 gives the exact value of $e_{{}^2A_2(q)}$ and $e_{{}^2B_2(q)}$, which can be extracted from [24] and [36]. We are now ready to prove Theorem 21.

*Proof of Theorem 21.*

Let $T, l, t, o, l_e, l_o$ and $e$ be as in the statement of Theorem 21. Given $e$ and $o$, write $(\dagger)_l$ for the inequality $l_o o^l > 6le^{3l/2} \log_2(e)$ in the variable $l$. We claim that if $(\dagger)_1$ holds (that is, $o > 6e^{3/2} \log_2(e)$), then $(\dagger)_l$ holds for every $l \geq 1$. Indeed,

$$l_o o^l \;\; > \;\; l_o(6e^{3/2} \log_2(e))^l \geq 6(6^{l-1} e^{3l/2} \log_2(e)^l) \geq 6le^{3l/2} \log_2(e)$$

where in the last inequality we used $6^{l-1} \geq l$. With a similar computation, it is easy to show that if $(\dagger)_2$ holds, then $(\dagger)_l$ holds for every $l \geq 2$. In particular, in order to show that $(\dagger)_l$ holds for every $l \geq 1$ (respectively $l \geq 2$), it suffices to prove that $(\dagger)_1$ (respectively $(\dagger)_2$) holds.

We divide the proof in different cases, depending on the isomorphism class of the non-abelian simple group $T$.

CASE $T$ IS A SPORADIC SIMPLE GROUP. As $|\mathrm{Aut}(T) : T| \leq 2$ for every sporadic simple group $T$, we get $e \leq 2^\varepsilon e_T$ with $\varepsilon = 1$ if $|\mathrm{Out}(T)| = 2$ and $\varepsilon = 0$ otherwise. Using [5,

| Group | $q$ odd | $q$ even | Reference |
|---|---|---|---|
| $A_{2n}$ | $2^{2n}$ | $q^{n(n+1)}$ | [1] |
| $A_{2n+1}$ | $2^{2n+2}$ | $q^{(n+1)^2}$ | [1] |
| $B_n, n \geq 2$ | $2^{2n}$ | $q^{n(n+1)/2}$ | [1] |
| $C_n, n \geq 3$ | $2^{2n}$ | $q^{n(n+1)/2}$ | [1] |
| $D_n, n \geq 4$ | $2^{2n}$ | $q^{n(n-1)/2}$ | [1] |
| $E_6$ | $2^{26}$ | $q^{16}$ | [31] |
| $E_7$ | $2^{56}$ | $q^{27}$ | [31] |
| $E_8$ | $2^{248}$ | $q^{36}$ | [31] |
| $F_4$ | $2^{26}$ | $q^{11}$ | [31] |
| $G_2$ | $2^6$ | $q^3$ | [31] |
| ${}^2A_2$ | $2^2$ | $q$ | [36] |
| ${}^2A_{2n}$ | $2^{2n}$ | $q^{n^2+1}$ | [36] |
| ${}^2A_{2n+1}, n \geq 1$ | $2^{2n+2}$ | $q^{(n+1)^2}$ | [36] |
| ${}^2B_2$ | - | $q$ | [24] |
| ${}^2D_n, n \geq 5$ | $2^{2n}$ | $q^{(n-1)(n-2)/2+2}$ | [35] |
| ${}^2D_4$ | $2^8$ | $q^6$ | [35] |
| ${}^3D_4$ | $2^8$ | $q^5$ | [31] |
| ${}^2E_6$ | $2^{26}$ | $q^{12}$ | [31] |
| ${}^2F_4$ | - | $q^5$ | [31] |
| ${}^2G_2$ | $2^3$ | - | [21] |

Table 4: Upper bound for $e_T$ for groups of Lie type

Table 1, page viii] and Table 3, it is immediate to check that, if $T \neq M_{12}$ and $M_{22}$, then $(\dagger)_1$ holds. It remains to consider the case that $T = M_{12}$ or $M_{22}$. If $T = M_{12}$, then, with `Magma`, we see that $e = 16$ and $(\dagger)_2$ holds. Similarly, if $T = M_{22}$, then, with `Magma`, we see that $e = 32$ and $(\dagger)_2$ holds.

CASE $T = \mathrm{Alt}(n)$. If $n = 5$, then $\mathrm{Aut}(T) = \mathrm{Sym}(5)$, $o = 15$, $e = 4$ and $6le^{3l/2}\log_2(e) = 12l8^l$. It is easy to show that $l_o 15^l > 12l8^l$ for $l \geq 5$. Therefore $(\dagger)_l$ holds for $l \geq 5$. If $n = 6$, then $\mathrm{Aut}(T) = \mathrm{P\Gamma L}(2, 9)$, $o = 45$, $e = 8$ and $6le^{3l/2}\log_2(e) = 18l8^{3l/2}$. It is easy to show that $l_o 45^l > 18l8^{3l/2}$ for $l \geq 5$. Therefore $(\dagger)_l$ holds for $l \geq 5$. If $n = 7$, then $o = 315$, $e = 8$ and $o^2 > 12e^3\log_2(e)$, hence $(\dagger)_l$ holds for every $l \geq 2$. If $n = 8$, then $o = 315$, $e = 16$ and $l_o o^l > 6le^{3l/2}\log_2(e)$ for $l \geq 3$. It follows that $(\dagger)_l$ holds for $l \geq 3$. From now on, we assume that $n \geq 9$. In particular, we have $\mathrm{Aut}(T) = \mathrm{Sym}(n)$ and, by Lemma 24, $e = 2^{\lfloor n/2 \rfloor}$. It follows that $6e^{3/2}\log_2(e) \leq 6\lfloor n/2 \rfloor 2^{3n/4}$. It is immediate to check that $o > 6\lfloor n/2 \rfloor 2^{3n/4}$ and hence $(\dagger)_1$ holds.

It remains to deal with the case of groups of Lie type. We follow [5] for notation and terminology, although we sometimes write $\mathrm{PSL}(n+1, q)$ instead of $A_n(q)$ when we need to emphasise some elementary property of the projective special linear group. Let $T$ be a group of Lie type over the base field of order $q = p^f$, where $p$ is a prime. We refer

to [5, Table 5, page xvi] for information about $|T|$ and $|\mathrm{Out}(T)|$. The outer automorphism group of $T$ is the semidirect product (in this order) of groups of order $d$ (the *diagonal* automorphisms), $f$ (the *field* automorphisms) and $g$ (the *graph* automorphisms of the corresponding Dynkin diagram), except when $T$ is one of $B_2(2^f)$, $G_2(3^f)$ or $F_4(2^f)$, in which case the *extraordinary* graph automorphism squares to a generator of the field automorphisms. The groups of order $d$, $f$ and $g$ are cyclic, except when $T = D_4(q)$, in which case the group of graph automorphisms is $\mathrm{Sym}(3)$. We use these facts later.

Write $\varepsilon_d = 1$ if $d$ is even and $\varepsilon_d = 0$ if $d$ is odd. Similarly, write $\varepsilon_f = 1$ if $f$ is even and $\varepsilon_f = 0$ if $f$ is odd. In the sequel, we will make use of the upper bounds for $e_T$ appearing in Table 4. The lower bounds for $|T|$ are obtained by using the inequality $q^i - 1 \geq q^{i-1}$ for $i \geq 1$. For instance, $|A_1(q)| = (q+1)q(q-1)/(2, q-1) \geq q^2$.

CASE $T = A_1(q)$, $q = p^f$. We have $|T| = q(q^2 - 1)/d$ with $d = (2, q-1)$. Also, $|\mathrm{Out}(T)| = df$.

SUBCASE $p = 2$. As $A_1(2)$ is soluble and $A_1(4) = \mathrm{Alt}(5)$, we may assume that $f \geq 3$. Clearly, $d = 1$. An elementary abelian subgroup of $\mathrm{Aut}(T) = \mathrm{P\Gamma L}(2, q)$ has order at most $2^{f+\varepsilon_f}$. As a Sylow 2-subgroup of $T$ is elementary abelian and has order $2^f$, we have $2^f \leq e$ and hence $2^f \leq e \leq 2^{f+\varepsilon_f}$. Now, we show that $e = 2^f$. If $f$ is odd, then $\varepsilon_f = 0$ and hence there is nothing to prove. Assume that $f$ is even. We argue by contradiction and we assume that $\mathrm{P\Gamma L}(2, q)$ contains an elementary abelian 2-subgroup $E$ of order $2^{f+1}$. As $\mathrm{Out}(T)$ is cyclic, the group $Q = E \cap T$ has order $2^f$ and hence is a Sylow 2-subgroup of $T$. Since $Q$ is self-centralising in $\mathrm{P\Gamma L}(2, q)$, we get $E \leq C_{\mathrm{P\Gamma L}(2,q)}(Q) = Q$, which is a contradiction.

From the previous paragraph, we have $e = q$ and $6e^{3/2}\log_2(e) = 6q^{3/2}f$. It is easy to check that $l_o(q^2 - 1)^l > 6lq^{3l/2}f$ if and only if $f \geq 13$ and $l \geq 1$, or $f \geq 7$ and $l = 2$, or $f \geq 3$ and $l = 3$, or $l = 4$ and $f \geq 4$, or $l \geq 5$.

SUBCASE $p > 2$. Clearly, $d = 2$. As $A_1(3)$ is soluble, $A_1(5) = A_1(4)$, $A_1(7) = A_2(2)$ (which we shall study later) and $A_1(9) = \mathrm{Alt}(6)$, we may assume that $q \neq 3, 5, 7, 9$. An elementary abelian subgroup of $\mathrm{Aut}(T) = \mathrm{P\Gamma L}(2, q)$ has order at most $2^{2+\varepsilon_f}$. Thence $6e^{3/2}\log_2(e) = 48 \cdot 2^{3\varepsilon_f/2}(2 + \varepsilon_f)$. Also, as $(q+1, q-1) = 2$, we have $o \geq q(q-1)/2$. For $(p, f) \neq (5, 2), (11, 1), (13, 1)$, we have $q(q-1)/2 > 48 \cdot 2^{3\varepsilon_f/2}(2 + \varepsilon_f)$ and $(\dagger)_1$ holds. If $T = A_1(11)$ or $A_1(13)$, we have $e = 4$, $(q(q-1)/2)^2 > 12e^3\log_2(e)$ and hence $(\dagger)_2$ holds. If $T = A_1(25)$, we have $e = 8$, $(q(q-1)/2)^2 > 12e^3\log_2(e)$ and hence $(\dagger)_2$ holds.

CASE $T = A_n(q)$, $q = p^f$, $n \geq 2$. We have $|T| = q^{n(n+1)/2}\prod_{i=1}^{n}(q^{i+1} - 1)/d$ with $d = (n+1, q-1)$. Also, $|\mathrm{Out}(T)| = df2$.

SUBCASE $p = 2$. Clearly, $d$ is odd and hence $e_{\mathrm{Out}(T)} \leq 2^{1+\varepsilon_f}$. Assume $n = 2m$. Since an elementary abelian subgroup of $T$ has order at most $q^{m(m+1)}$, we get $e \leq 2^{1+\varepsilon_f}q^{m(m+1)}$. Using this inequality, for $(f, m) \neq (1, 1), (1, 2), (2, 1), (3, 1)$ and $(4, 1)$, we have $o >$

$6e^{3/2}\log_2(e)$ and $(\dagger)_1$ holds. For $(f,m)=(1,1)$, we have $T=A_2(2)$ and, with `Magma`, we see that $e=4$, $o=21$ and $l_o o^l > 6le^{3l/2}\log_2(e)$ for every $l\neq 1,2,4$. For $(f,m)=(2,1)$, we have $T=A_2(4)$ and, with `Magma`, we see that $e=2^4$, $o=315$ and $l_o o^l > 6le^{3l/2}\log_2(e)$ for every $l\geq 3$. For $(f,m)=(3,1)$, we have $T=A_2(8)$ and, with `Magma`, we see that $e=2^6$ and $o>6e^{3/2}\log_2(e)$, hence $(\dagger)_1$ holds. For $(f,m)=(4,1)$, we have $T=A_2(16)$ and, with `Magma`, we see that $e=2^8$ and $o>6e^{3/2}\log_2(e)$, hence $(\dagger)_1$ holds. For $(f,m)=(1,2)$, we have $T=A_4(2)$ and, with `Magma`, we see that $e=2^6$ and $o^2>12e^3\log_2(e)$, hence $(\dagger)_2$ holds.

Assume $n=2m+1$. As $A_3(2)=\mathrm{Alt}(8)$, we may assume that $(m,f)\neq(1,1)$. Since an elementary abelian subgroup of $T$ has order at most $q^{(m+1)^2}$ and $e_{\mathrm{Out}(T)}\leq 2^{1+\varepsilon_f}$, we get $e\leq 2^{1+\varepsilon_f}q^{(m+1)^2}$. Using this inequality, for $(f,m)\neq(1,2)$ and $(2,1)$, we have $o>6e^{3/2}\log_2(e)$ and $(\dagger)_1$ holds. For $(f,m)=(2,1)$, we have $T=A_3(4)$ and, with `Magma`, we see that $e=2^8$ and $o>6e^{3/2}\log_2(e)$, hence $(\dagger)_1$ holds. For $(f,m)=(1,2)$, we have $T=A_5(2)$ and, with `Magma`, we see that $e=2^9$ and $o^2>12e^3\log_2(e)$, hence $(\dagger)_2$ holds.

SUBCASE $p>2$. From Lemma 25, we obtain $e_{\mathrm{PGL}(n+1,q)}=2^{n+1}$. Furthermore, $|\mathrm{Aut}(T):\mathrm{PGL}(n+1,q)|=2f$. Hence $e\leq 2^{n+2+\varepsilon_f}$. Using this inequality, it is easy to check that, for $(q,n)\neq(3,2)$, we have $o>6e^{3/2}\log_2(e)$ and hence $(\dagger)_1$ holds. For $(q,n)=(3,2)$, we have $T=A_2(3)$ and, with `Magma`, we see that $e=8$, $o=351$ and $o^2>12e^3\log_2(e)$, hence $(\dagger)_2$ holds.

CASE $T=B_2(q)$, $q=p^f$. We have $|T|=q^4(q^4-1)(q^2-1)/d$ with $d=(2,q-1)$. Also, $|\mathrm{Out}(T)|=df2$ if $p=2$ (in which case the subgroup of $\mathrm{Out}(T)$ corresponding to $f2$ is cyclic, see [5, page xv]) and $|\mathrm{Out}(T)|=df$ if $p\neq 2$.

SUBCASE $p=2$. Clearly, $d=1$. Since $B_2(2)=\mathrm{Sym}(6)$, we may assume that $f\geq 2$. As an elementary abelian 2-subgroup of $T$ has order at most $q^3$, we have $e\leq 2q^3$. Using this inequality, for every $f\geq 6$, we get $(q^4-1)(q^2-1)>6e^{3/2}\log_2(e)$ and hence $(\dagger)_1$ holds. Also, using again $e\leq 2q^3$, for $f=4,5$, we obtain $((q^4-1)(q^2-1))^2>12e^3\log_2(e)$ and hence $(\dagger)_2$ holds. If $f=3$, then, with `Magma`, we see that $e=2^9$. Now, with a direct computation, we see that $o^2>12e^3\log_2(e)$ and hence $(\dagger)_2$ holds. Finally, if $f=2$, then, with `Magma`, we see that $e=2^6$. Using this value for $e$, it is easy to check with a direct computation that $(\dagger)_l$ holds for every $l\geq 3$.

SUBCASE $p>2$. Clearly, $d=2$. Also, as $(q^2-1,q^2+1)=2$, we have $o>q^4(q^2-1)/2$. Since $B_2(q).d=\mathrm{PSp}(4,q).d\leq\mathrm{PGL}(4,q)$, from Lemma 25 we obtain $e_{B_2(q).d}=2^4=16$. Therefore, $e\leq 2^{4+\varepsilon_f}$. Using this inequality, for $q\geq 5$, we have that $o\geq 5^4(5^2-1)/2>6e^{3/2}\log_2(e)$ and hence $(\dagger)_1$ holds. Assume $q=3$. With `Magma`, we see that $e=16$, $o=405$ and $(\dagger)_l$ holds for every $l\geq 3$.

CASE $T=B_n(q)$, $q=p^f$, $n\geq 3$. We have $|T|=q^{n^2}\prod_{i=1}^n(q^{2i}-1)/d$ with $d=(2,q-1)$. Also, $|\mathrm{Out}(T)|=df$.

SUBCASE $p = 2$. Clearly, $d = 1$ and $o = \prod_{i=1}^{n}(q^{2i} - 1)$. As an elementary abelian 2-subgroup of $T$ has order at most $q^{n(n+1)/2}$, we have $e \leq 2^{\varepsilon_f} q^{n(n+1)/2}$. Using this inequality, it is easy to verify that for $n \geq 5$, we have $o > 6e^{3/2}\log_2(e)$ and hence $(\dagger)_1$ holds.

For the remaining values of $n$ (that is, $n \in \{3, 4\}$), we get that $o > 6e^{3/2}\log_2(e)$ if and only if $n = 4$ and $f > 1$, or $n = 3$ and $f > 2$. In particular, it remains to study the groups $B_3(2), B_3(4)$ and $B_4(2)$. If $T = B_3(2)$, then, with `Magma`, we see that $e = 2^6$, $o = 2835$ and $l_o o^l > 6le^{3l/2}\log_2(e)$ for every $l \geq 3$. If $T = B_3(4)$, then, with `Magma`, we see that $e = 4^6$, $o = 15663375$ and $o^2 > 12e^3\log_2(e)$, hence $(\dagger)_2$ holds. Similarly, if $T = B_4(2)$, then, with `Magma`, we see that $e = 2^{10}$ and $o^2 > 12e^3\log_2(e)$, hence $(\dagger)_2$ holds.

SUBCASE $p > 2$. Clearly, $d = 2$. Since $(q^n - 1, q^n + 1) = 2$, we have $o \geq q^{n^2}(q^n - 1)/2 \geq 3^{n^2}(3^n - 1)/2$. As an elementary abelian subgroup of $T$ has order at most $2^{2n}$ and $e_{\mathrm{Out}(T)} \leq 2^{1+\varepsilon_f}$, we have $e \leq 2^{2n+1+\varepsilon_f} \leq 2^{2n+2}$. Using this inequality, we get $o \geq 3^{n^2}(3^n - 1)/2 > 6e^{3/2}\log_2(e)$ and $(\dagger)_1$ holds.

CASE $T = C_n(q)$, $q = p^f$. We have $|T| = q^{n^2}\prod_{i=1}^{n}(q^{2i} - 1)/d$ with $d = (2, q - 1)$ and $n \geq 3$. Also, $|\mathrm{Out}(T)| = df$.

SUBCASE $p = 2$. We have $B_n(q) = C_n(q)$ and there is nothing to prove.

SUBCASE $p > 2$. This subcase is exactly as the subcase $B_n(q)$ with $q$ odd.

CASE $T = D_n(q)$, $q = p^f$. We have $|T| = q^{n(n-1)}(q^n - 1)\prod_{i=1}^{n-1}(q^{2i} - 1)/d$ with $d = (4, q^n - 1)$ and $n \geq 4$. Also, $|\mathrm{Out}(T)| = df6$ if $n = 4$ and $|\mathrm{Out}(T)| = df2$ if $n > 4$. In particular, $e_{\mathrm{Out}(T)} = 2^{1+\varepsilon_d+\varepsilon_f}$.

SUBCASE $p = 2$. Clearly, $d = 1$ and $o \geq (q^n - 1)\prod_{i=1}^{n-1} q^{2i-1} = (q^n - 1)q^{(n-1)^2}$. As an elementary abelian 2-subgroup of $T$ has order at most $q^{n(n-1)/2} = 2^{n(n-1)f/2}$, we have $e \leq 2^{n(n-1)f/2+1+\varepsilon_f}$. It follows that $6e^{3/2}\log_2(e) \leq 6 \cdot 2^{3/2+3\varepsilon_f/2}(n(n-1)f/2 + 1 + \varepsilon_f)q^{3n(n-1)/4}$. Now, it is easy to verify that for $n \geq 6$, we have $(q^n - 1)q^{(n-1)^2} > 6 \cdot 2^{3/2+3\varepsilon_f/2}(n(n-1)f/2 + 1 + \varepsilon_f)q^{3n(n-1)/4}$ and hence $(\dagger)_1$ holds.

For the remaining values of $n$ (that is, $n \in \{4, 5\}$), using the explicit formula for $|T|$ we get that $o > 6 \cdot 2^{3/2+3\varepsilon_f/2}(n(n-1)f/2 + 1 + \varepsilon_f)q^{3n(n-1)/4}$ if and only if $n = 5$, or $n = 4$ and $f > 1$. In particular, it remains to study the group $T = D_4(2)$. Using `Magma`, we see that $e = 2^7$, that $(\dagger)_1$ fails and that $o^2 > 12e^3\log_2(e)$. It follows that $(\dagger)_l$ holds for $l \geq 2$.

SUBCASE $p > 2$. Clearly, $d$ is even and $o > q^{n(n-1)}$. As an elementary abelian 2-subgroup of $T$ has order at most $2^{2n}$, we have $e \leq 2^{2+\varepsilon_f} \cdot 2^{2n} = 2^{2n+2+\varepsilon_f}$. Using this inequality it is easy to see that for $q \geq 5$, we get $o > 5^{n(n-1)} > 6e^{3/2}\log_2(e)$ and $(\dagger)_1$ holds. Finally, for $q = 3$ using that $o \geq 5 \cdot 3^{n(n-1)}$, we obtain $o > 6e^{3/2}\log_2(e)$ and hence $(\dagger)_1$ holds.

CASE $T = E_6(q)$, $q = p^f$. We have $|T| = q^{36}(q^{12} - 1)(q^9 - 1)(q^8 - 1)(q^6 - 1)(q^5 - 1)(q^2 - 1)/d$ with $d = (3, q - 1)$. Also, $|\mathrm{Out}(T)| = df2$.

SUBCASE $p = 2$. Clearly, $d$ is odd and $o > q^{36}$. As an elementary abelian 2-subgroup of $T$ has order at most $q^{16} = 2^{16f}$, we get $e \leq 2^{1+\varepsilon_f} \cdot q^{16} = 2^{16f+1+\varepsilon_f}$. It follows that

$6e^{3/2}\log_2(e) \le 6\cdot 2^{3/2+3\varepsilon_f/2}q^{24}(16f+1+\varepsilon_f)$. Now, $o > q^{36} > 6\cdot 2^{3/2+3\varepsilon_f/2}q^{24}(16f+1+\varepsilon_f)$ and hence $(\dagger)_1$ holds.

SUBCASE $p > 2$. Clearly, $d$ is odd and $o \ge q^{36}$. As an elementary abelian $2$-subgroup of $T$ has order at most $2^{26}$, we get $e \le 2^{1+\varepsilon_f}\cdot 2^{26} \le 2^{28}$. Now, $o \ge q^{36} \ge 3^{36} > 6e^{3/2}\log_2(e)$ and hence $(\dagger)_1$ holds.

CASE $T = E_7(q)$, $q = p^f$. We have $|T| = q^{63}(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^{10}-1)(q^8-1)(q^6-1)(q^2-1)/d$ with $d = (2, q-1)$. Also, $|\mathrm{Out}(T)| = df$.

SUBCASE $p = 2$. Clearly, $d = 1$ and $o > q^{63}$. An elementary abelian $2$-subgroup of $T$ has order at most $q^{27} = 2^{27f}$. Therefore $e \le 2^{\varepsilon_f}q^{27} = 2^{27f+\varepsilon_f}$. It follows that $6e^{3/2}\log_2(e) \le 6(2q^{27})^{3/2}(27f+1)$. Using this inequality, it is easy to check that $q^{63} > 6e^{3/2}\log_2(e)$ and hence $(\dagger)_1$ holds.

SUBCASE $p > 2$. Clearly, $d = 2$ and $o \ge q^{63}$. As an elementary abelian $2$-subgroup of $T$ has order at most $2^{56}$, we get $e \le 2^{1+\varepsilon_f}\cdot 2^{56} \le 2^{58}$. Now, $o \ge q^{63} \ge 3^{63} > 6e^{3/2}\log_2(e)$ and hence $(\dagger)_1$ holds.

CASE $T = E_8(q)$, $q = p^f$. We have $|T| = q^{120}(q^{30}-1)(q^{24}-1)(q^{20}-1)(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^8-1)(q^2-1)$. Also, $|\mathrm{Out}(T)| = f$.

SUBCASE $p = 2$. Clearly, $o > q^{120}$. An elementary abelian $2$-subgroup of $T$ has order at most $q^{36} = 2^{36f}$. Therefore $e \le 2^{\varepsilon_f}\cdot q^{36} = 2^{36f+\varepsilon_f}$. It follows that $6e^{3/2}\log_2(e) \le 6\cdot 2^{3\varepsilon_f/2}q^{54}(36f+\varepsilon_f)$. Now, $o > q^{120} > 6\cdot 2^{3\varepsilon_f/2}q^{54}(36f+\varepsilon_f)$ and hence $(\dagger)_1$ holds.

SUBCASE $p > 2$. Note that $(q^{4n+2}-1) = (q^2-1)(q^{4n}+q^{4n-2}+\cdots+q^2+1)$ and $q^{4n}+q^{4n-2}+\cdots+q^2+1$ is odd (because it is the sum of $(2n+1)$ odd summands). Hence the higher power of $2$ dividing $q^{4n+2}-1$ is at most $q^2-1$. Using the formula for $|T|$ and this remark, we obtain that a Sylow $2$-subgroup of $T$ has order at most $(q^2-1)^4(q^{24}-1)(q^{20}-1)(q^{12}-1)(q^8-1) < q^{2\cdot 4+24+20+12+8} = q^{72}$. It follows that $6e^{3/2}\log_2(e) \le 6(2q^{72})^{3/2}\log_2(2q^{72})$. Using this inequality, we obtain $o > q^{120} > 6e^{3/2}\log_2(e)$ and hence $(\dagger)_1$ holds.

CASE $T = F_4(q)$, $q = p^f$. We have $|T| = q^{24}(q^{12}-1)(q^8-1)(q^6-1)(q^2-1)$. Also, $|\mathrm{Out}(T)| = f2$ if $p = 2$ (in which case $\mathrm{Out}(T)$ is cyclic, see [5, page xv]) and $|\mathrm{Out}(T)| = f$ if $p > 2$.

SUBCASE $p = 2$. Clearly, $o > q^{24}$. As an elementary abelian $2$-subgroup of $T$ has order at most $q^{11} = 2^{11f}$ and $\mathrm{Out}(T)$ is cyclic, we get $e \le 2q^{11} = 2^{11f+1}$. Using this inequality, for $f \ge 2$ we obtain $o > q^{24} > 6e^{3/2}\log_2(e)$ and hence $(\dagger)_1$ holds. If $f = 1$, then using the explicit value for $o$ we also obtain $o > 6e^{3/2}\log_2(e)$ and hence $(\dagger)_1$ holds.

SUBCASE $p > 2$. As an elementary abelian $2$-subgroup of $T$ has order at most $2^{26}$, we get $e \le 2^{\varepsilon_f}\cdot 2^{26} \le 2^{27}$. For $q \ge 5$, we have $o \ge 5^{24} > 6\cdot(2^{27})^{3/2}\cdot 27$ and hence $(\dagger)_1$ holds. Finally, if $q = 3$, then using the explicit value of $o$ we also obtain $o > 6\cdot(2^{27})^{3/2}\cdot 27$ and hence $(\dagger)_1$ holds.

CASE $T = G_2(q)$, $q = p^f$. We have $|T| = q^6(q^6-1)(q^2-1)$. Also, $|\mathrm{Out}(T)| = f$ if

$p \neq 3$ and $|\mathrm{Out}(T)| = f2$ if $p = 3$.

SUBCASE $p = 2$. As $G_2(2)$ is not simple and $G_2(2)' = {}^2A_2(3)$ (which we shall study later), we may assume $f \geq 2$. As an elementary abelian $2$-subgroup of $T$ has order at most $q^3 = 2^{3f}$, we get $e \leq 2^{\varepsilon_f} \cdot q^3 = 2^{3f+\varepsilon_f}$. It follows that $6e^{3/2}\log_2(e) \leq 6 \cdot 2^{3\varepsilon_f/2} \cdot q^{9/2} \cdot (3f + \varepsilon_f)$. Now, $o = (q^6 - 1)(q^2 - 1) > 6 \cdot 2^{3\varepsilon_f/2} \cdot q^{9/2} \cdot (3f + \varepsilon_f)$ and hence $(\dagger)_1$ holds.

SUBCASE $p > 2$. Assume $q > 3$. As an elementary abelian $2$-subgroup of $T$ has order at most $2^6$, we get $e \leq 2^{1+\varepsilon_f} \cdot 2^6 \leq 2^8$. Since $(q^3 - 1, q^3 + 1) = 2$, we have $o \geq q^6(q^3 - 1)/2$. Now, $o \geq 5^6(5^3 - 1)/2 > 6 \cdot (2^8)^{3/2} \cdot 8$ and hence $(\dagger)_1$ holds. Finally, assume $q = 3$. Using `Magma`, we see that $e = 16$, $o = 66339$ and $o > 6e^{3/2}\log_2(e)$ and hence $(\dagger)_1$ holds.

CASE $T = {}^2A_n(q)$, $q = p^f$. We have $|T| = q^{n(n+1)/2}\prod_{i=1}^{n}(q^{i+1} - (-1)^{i+1})/d$ with $n \geq 2$ and $d = (n+1, q+1)$. Also, $|\mathrm{Out}(T)| = df2$ and the subgroup of $\mathrm{Out}(T)$ corresponding to $f2$ is cyclic (being the Galois group of the defining field for the unitary group $T$). Therefore $e_{\mathrm{Out}(T)} \leq 2^{1+\varepsilon_d}$. Recall that ${}^2A_2(2)$ is soluble and ${}^2A_3(2) = B_2(3)$.

SUBCASE $p = 2$. Clearly $d$ is odd. Assume $n = 2m + 1$. As an elementary abelian $2$-subgroup of $T$ has order at most $q^{(m+1)^2}$, we get $e \leq 2q^{(m+1)^2}$. Using this inequality, for $(m, f) \neq (1, 1), (1, 2)$ and $(2, 1)$, we have $o > 6e^{3/2}\log_2(e)$ and hence $(\dagger)_1$ holds. Also, as ${}^2A_3(2) \cong B_2(3)$ and we have already studied $B_2(3)$, we may assume that $(m, f) \neq (1, 1)$. Assume $T = {}^2A_3(4)$. With `Magma`, we see that $e = 2^8$. As $o > 6e^{3/2}\log_2(e)$, we obtain that $(\dagger)_1$ holds. Assume $T = {}^2A_5(2)$. With `Magma`, we see that $e = 2^9$. As $o^2 > 12e^3\log_2(e)$, we obtain that $(\dagger)_2$ holds.

Now, assume $n = 2$. As an elementary abelian $2$-subgroup of $T$ has order at most $q$, we get $e \leq 2q = 2^{1+f}$. Using this inequality, we have $o > 6e^{3/2}\log_2(e)$ and $(\dagger)_1$ holds.

Finally, assume $n = 2m$ with $m > 1$. As an elementary abelian $2$-subgroup of $T$ has order at most $q^{m^2+1}$, we get $e \leq 2q^{m^2+1} = 2^{1+f+m^2f}$. Using this inequality, for $(m, f) \neq (2, 1)$ we have $o > 6e^{3/2}\log_2(e)$ and $(\dagger)_1$ holds. If $T = {}^2A_4(2)$, then we see, with `Magma`, that $e = 16$ and $o > 6e^{3/2}\log_2(e)$ and hence $(\dagger)_1$ holds.

SUBCASE $p > 2$. As an elementary abelian $2$-subgroup of $T$ has order at most $2^{n+1}$, we get $e \leq 2^{n+2+\varepsilon_d}$ and $6e^{3/2}\log_2(e) \leq 3 \cdot 2^{3n/2+4+3\varepsilon_d/2}(n + 2 + \varepsilon_d)$. With this inequality, we have that, for $(n, q) \neq (2, 3)$, the inequality $(\dagger)_1$ holds. Assume $T = {}^2A_2(3)$. Clearly, $d = 1$ and $o = 189$. With `Magma`, we see that $e = 8$. Now, $o^2 > 12e^3\log_2(e)$ and hence $(\dagger)_2$ holds.

CASE $T = {}^2B_2(q)$, $q = 2^{2m+1}$. We have $|T| = q^2(q^2+1)(q-1)$. Since ${}^2B_2(2)$ is soluble, we may assume that $m \geq 1$. We have $|\mathrm{Out}(T)| = 2m+1$ and hence an elementary abelian $2$-subgroup of $\mathrm{Aut}(T)$ is contained in $T$. A maximal elementary abelian $2$-subgroup of $T$ has order $q$. Therefore $e = q$ and $6e^{3/2}\log_2(e) = 6q^{3/2}(2m + 1)$. It is easy to check that $o = (q^2 + 1)(q - 1) > 6q^{3/2}(2m + 1)$ and hence $(\dagger)_1$ holds.

CASE $T = {}^2D_n(q)$, $q = p^f$. We have $n \geq 4$ and $|T| = q^{n(n-1)}(q^n + 1)\prod_{i=1}^{n-1}(q^{2i} - 1)/d$

with $d=(4,q^n+1)$. Also, $|\mathrm{Out}(T)|=df2$.

SUBCASE $p=2$. Clearly, $d=1$. Assume $n=4$. An elementary abelian 2-subgroup of $T$ has order at most $q^6$. Hence $e\leq 2^{1+\varepsilon_f}q^6$ and $6e^{3/2}\log_2(e)\leq 6\cdot 2^{3/2+3\varepsilon_f/2}q^9(6f+1+\varepsilon_f)$. With this inequality, it is easy to check that $(\dagger)_1$ holds for $f\geq 2$. If $f=1$, then $o=48195$, $e\leq 2^7$ and $o^2>12e^3\log_2(e)$ and hence $(\dagger)_2$ holds.

Assume $n\geq 5$. An elementary abelian 2-subgroup of $T$ has order at most $q^{(n-1)(n-2)/2+2}$. Hence $e\leq 2^{1+\varepsilon_f}q^{(n-1)(n-2)/2+2}$. With this inequality, it is easy to check that $o>q^{(n-1)^2+n}>6e^{3/2}\log_2(e)$ and hence $(\dagger)_1$ holds.

SUBCASE $p>2$. An elementary abelian 2-subgroup of ${}^2D_n(q)$ has order at most $2^{2n}$ and hence $e\leq 2^{2n+1+\varepsilon_d+\varepsilon_f}\leq 2^{2n+3}$. With this inequality, it is easy to prove (for $(n,q)\neq(4,3)$) that $o>q^{n(n-1)}>6e^{3/2}\log_2(e)$ and hence $(\dagger)_1$ holds. If $(n,q)=(4,3)$, we have $\varepsilon_f=0$ and $e\leq 2^{10}$. With a direct computation we see that $o>6e^{3/2}\log_2(e)$ and hence $(\dagger)_1$ holds.

CASE $T={}^3D_4(q)$, $q=p^f$. We have $|T|=q^{12}(q^8+q^4+1)(q^6-1)(q^2-1)$ and $|\mathrm{Out}(T)|=3f$.

SUBCASE $p=2$. As an elementary abelian 2-subgroup of $T$ has order at most $q^5$, we get $e\leq 2^{\varepsilon_f}q^5$ and $6e^{3/2}\log_2(e)\leq 6\cdot 2^{3\varepsilon_f/2}q^{15/2}(5f+\varepsilon_f)$. With this inequality it is easy to check that $o>q^{14}>6\cdot 2^{3\varepsilon_f/2}q^{15/2}(5f+\varepsilon_f)$ and hence $(\dagger)_1$ holds.

SUBCASE $p>2$. As an elementary abelian 2-subgroup of $T$ has order at most $2^8$, we get $e\leq 2^{8+\varepsilon_f}\leq 2^9$. Now, $o\geq 3^{12}(3^8+3^4+1)>6\cdot 2^{27/2}\cdot 9\geq 6e^{3/2}\log_2(e)$ and hence $(\dagger)_1$ holds.

CASE $T={}^2E_6(q)$, $q=p^f$. We have $|T|=q^{36}(q^{12}-1)(q^9+1)(q^8-1)(q^6-1)(q^5+1)(q^2-1)/d$ with $d=(3,q+1)$. Also, $|\mathrm{Out}(T)|=df2$.

SUBCASE $p=2$. Clearly, $d$ is odd. A maximal elementary abelian 2-subgroup of $T$ has order at most $q^{12}=2^{12f}$. Therefore $e\leq 2^{1+\varepsilon_f}q^{12}=2^{12f+1+\varepsilon_f}$. It follows that $6e^{3/2}\log_2(e)\leq 6\cdot 2^{3/2+3\varepsilon_f/2}\cdot q^{18}\cdot(12f+1+\varepsilon_f)$. With this inequality it is easy to check that $(\dagger)_1$ holds.

SUBCASE $p>2$. Clearly, $d$ is odd. A maximal elementary abelian 2-subgroup of $T$ has order at most $2^{26}$. Therefore $e\leq 2^{1+\varepsilon_f}2^{26}\leq 2^{28}$. It follows that $6e^{3/2}\log_2(e)\leq 6\cdot 2^{42}\cdot 28$. With this inequality it is easy to check that $o>3^{36}>6\cdot 2^{42}\cdot 28$ and hence $(\dagger)_1$ holds.

CASE $T={}^2F_4(q)$, $q=2^{2m+1}$. For $m\geq 1$, we have $|T|=q^{12}(q^6+1)(q^4-1)(q^3+1)(q-1)$. Also, $|\mathrm{Out}(T)|=f=2m+1$ and hence an elementary abelian 2-subgroup of $\mathrm{Aut}(T)$ is contained in $T$ and has order at most $q^5$. Hence $e\leq q^5$. It follows that $6e^{3/2}\log_2(e)\leq 6q^{15/2}(10m+5)$. For $m\geq 1$, we get $o\geq q^{12}>6q^{15/2}(10m+5)$ and hence $(\dagger)_1$ holds. If $m=0$, then ${}^2F_4(2)$ is not simple, the Tits group $T={}^2F_4(2)'$ is simple, $|{}^2F_4(2):{}^2F_4(2)'|=2$ and ${}^2F_4(2)=\mathrm{Aut}({}^2F_4(2)')$. With `Magma`, we see that $e=32$, $o>6\cdot 32^{3/2}\cdot 5$ and hence $(\dagger)_1$ holds.

CASE $T={}^2G_2(q)$, $q=3^{2m+1}$. We have $|T|=q^3(q^3+1)(q-1)$ and $|\mathrm{Out}(T)|=$

$2m+1$. Since ${}^2G_2(3)$ is not simple and ${}^2G_2(3)' = A_1(8)$, we may assume that $m \geq 1$. As $|\mathrm{Out}(T)|$ is odd, an elementary abelian $2$-subgroup of $\mathrm{Aut}(T)$ is contained in $T$. Since a Sylow $2$-subgroup of $T$ has order $8$, we get $e \leq 8$. It follows that $6e^{3/2}\log_2(e) \leq 408$. Now, $o \geq |{}^2G_2(27)|/8 > 408$ and hence $(\dagger)_1$ holds. $\square$

# 7 Additional remarks

## 7.1 Cubic vertex-transitive graphs

Tutte's theorem concerns the order of a vertex-stabiliser in a $3$-valent arc-transitive graph. Instead of trying to generalise it to valencies other than $3$, it is also possible to consider $3$-valent vertex-transitive graphs in general. It turns out that the problem of bounding the order of the vertex-stabiliser of a $3$-valent vertex-transitive graph is essentially equivalent to the problem of bounding it for 4-valent arc-transitive graphs. We now give a brief explanation of this possibly surprising fact. Let $(\Gamma, G)$ be a locally-$L$ pair such that $\Gamma$ has valency 3. If $L$ is transitive, then $\Gamma$ is $G$-arc-transitive and, by Tutte's theorem, $|G_v| \leq 48$. Similarly, if $L = 1$, then $G_v = 1$ because $\Gamma$ is connected. Since we are interested in graphs with 'large' vertex-stabilisers, we ignore both of these cases. In particular, we may assume that $L \cong \mathrm{C}_2^{[3]}$, where $\mathrm{C}_2^{[3]}$ denotes the permutation group of order 2 and degree 3.

For each locally-$\mathrm{C}_2^{[3]}$ pair $(\Gamma, G)$, we construct an auxiliary locally-$\mathrm{D}_4$ pair $(\mathrm{MG}(\Gamma), G)$. Conversely, for each locally-$\mathrm{D}_4$ pair $(\Gamma, G)$, we construct a locally-$\mathrm{C}_2^{[3]}$ pair $(\mathrm{SG}(\Gamma), G)$. Moreover, we will show that these constructions are inverses of each other.

**Definition 26.** Let $(\Gamma, G)$ be locally-$\mathrm{C}_2^{[3]}$. As $\mathrm{C}_2^{[3]}$ fixes a unique point, each vertex $v \in \mathrm{V}\Gamma$ has a unique neighbour $v' \in \Gamma(u)$ with $G_v = G_{v'}$. Hence the set of pairs $\Sigma = \{\{v, v'\} : v \in \mathrm{V}\Gamma\}$ forms a system of imprimitivity for $G$. Let $\mathrm{MG}(\Gamma) = \Gamma/\Sigma$.

**Definition 27.** Let $(\Gamma, G)$ be locally-$\mathrm{D}_4$. For every arc $a = (u, v)$ of $\Gamma$, there is a unique arc $a' = (u, w)$ such that $a$ and $a'$ have the same head and $G_a = G_{a'}$. Write $\overline{a} = \{a, a'\}$. We define a new graph $\mathrm{SG}(\Gamma)$ with vertices $\{\overline{a} : a \in \mathrm{A}\Gamma\}$ and two distinct elements $\overline{(u, v)}$ and $\overline{(w, x)}$ are adjacent if either $u = w$, or $u = x$ and $v = w$. Note that the set $\{\overline{a} : a \in \mathrm{A}\Gamma\}$ forms a system of imprimitivity for $G$.

**Lemma 28.** *Let $(\Gamma, G)$ be locally-$\mathrm{C}_2^{[3]}$ with $|G_v| \geq 4$. For a vertex $v \in \mathrm{V}\Gamma$, let $v'$ be the unique neighbour of $v$ with $G_v = G_{v'}$. Then $(\mathrm{MG}(\Gamma), G)$ is locally-$\mathrm{D}_4$, $\mathrm{MG}(\Gamma)$ has $|\mathrm{V}\Gamma|/2$ vertices and $|G_{\{v,v'\}}| = 2|G_v|$. Moreover, $\mathrm{SG}(\mathrm{MG}(\Gamma)) \cong \Gamma$, with the isomorphism given by $\theta : \overline{(\{u, u'\}, \{v, v'\})} \mapsto u$, where $u' \neq v \in \Gamma(u)$.*

*Proof.* It is clear from Definition 26 that $G$ acts transitively on the arcs of $\mathrm{MG}(\Gamma)$, which is connected and has $|\mathrm{V}\Gamma|/2$ vertices. For a vertex $v \in \mathrm{V}\Gamma$, let $K(v)$ denote the kernel of the action of $G_v$ on $\Gamma(v)$. Note that, if $u$ is adjacent to $v$ and $u \neq v'$, then $K(u) = K(v)$.

Suppose that $\Gamma$ contains a 3-cycle of the form $(u, v, v')$. Then $G_v$ fixes $v'$ and at least 2 neighbours of $v'$ hence $K(v) = K(v')$. If follows that $K(w) = K(v)$ for every neighbour $w \in \Gamma(v)$. Since $\Gamma$ is connected and $G$-vertex-transitive, we conclude that $K(v) = 1$ and hence $|G_v| = 2$, which is a contradiction. Now, suppose that $\Gamma$ contains a 4-cycle of the form $(u, u', v', v)$. Then, $G_v$ fixes $v$, $v'$, $u$ and, in particular, $u'$ hence $K(v) = K(v')$, which is a contradiction, for the same reasons as above.

Since $\Gamma$ contains no such cycles, it is easily seen that $G$ acts faithfully on the vertices of $\mathrm{MG}(\Gamma)$ and that $\mathrm{MG}(\Gamma)$ is 4-valent. It follows that $|G_{\{v,v'\}}| = 2|G_v| \geq 8$ and hence $(\mathrm{MG}(\Gamma), G)$ must be locally-$\mathrm{D}_4$. The proof that $\theta$ is a well-defined isomorphism is straightforward. $\square$

We also leave the proof of the next lemma to the reader.

**Lemma 29.** *Let* $(\Gamma, G)$ *be locally-*$\mathrm{D}_4$*. Then* $(\mathrm{SG}(\Gamma), G)$ *is locally-*$\mathrm{C}_2^{[3]}$*,* $\mathrm{SG}(\Gamma)$ *has* $2|\mathrm{V}\Gamma|$ *vertices and* $|G_{\overline{a}}| = |G_v|/2$*. Moreover,* $\mathrm{MG}(\mathrm{SG}(\Gamma)) \cong \Gamma$*, with the isomorphism given by* $\{\overline{(u,v)}, \overline{(u,v)}'\} \mapsto u$*.*

Combining Lemmas 28 and 29 with Theorem 2 yields Corollary 4.

## 7.2 Normal subgroups of Djoković's amalgams

In this section we will restate Theorem 2 in a purely group theoretical language. Following Djoković [7], we call a quintuple $(L, \varphi, B, \psi, R)$ an *amalgam* provided that $L, B$ and $R$ are finite groups and $\varphi : B \to L$, $\psi : B \to R$ are monomorphisms (the embeddings $\varphi$ and $\psi$ are often omitted from the notation when they are clear from the context). Amalgams are usually given by means of an ambient group $G$ (called a *completion of the amalgam*), containing $L$ and $R$ as subgroups with $B = L \cap R$, and where $\varphi$ and $\psi$ are the inclusion mappings. Note that, for each amalgam $(L, \varphi, B, \psi, R)$, there exists the *universal completion* $G^*$ (that is, the free product of $L$ and $R$ with amalgamation over $B$, and denoted by $L *_B R$), with the property that every other completion $G$ is a quotient of $G^*$ by some normal subgroup $N$ intersecting both $L$ and $R$ trivially. We shall call such a quotient $G^* \to G^*/N \cong G$ a *smooth quotient*. The *index* of the amalgam $(L, \varphi, B, \psi, R)$ is the pair $(|L : \varphi(B)|, |R : \psi(B)|)$. Finally, the amalgam is *faithful* if there is no nontrivial subgroup $H \leq B$ with $\varphi(H)$ and $\psi(H)$ normal in $L$ and $R$, respectively.

Amalgams emerge naturally in many different contexts and areas of mathematics [23] and have a natural interpretation in the context of arc-transitive graphs. Namely, if $\Gamma$ is a finite $G$-arc-transitive graph of valency $k$, then $(G_v, G_{uv}, G_{\{u,v\}})$ (with the monomorphisms being the inclusion mappings) is a faithful amalgam of index $(k, 2)$ and $G$ is a finite smooth quotient of the universal group $G_v *_{G_{uv}} G_{\{u,v\}}$. Conversely, given a finite smooth quotient $G \cong (L *_B R)/N$ of a faithful amalgam $(L, B, R)$ of index $(k, 2)$, one

can use the *coset graph* construction to obtain a finite $G$-arc-transitive graph. Note that in this correspondence, the stabiliser $G_v$ corresponds to the group $L$ and the permutation group $G_v^{\Gamma(v)}$ corresponds to the permutation group induced by the action of $L$ on the cosets of $B$ by right multiplication. If the latter permutation group is permutation isomorphic to $P$, we say that the amalgam $(L, B, R)$ is of *local type* $P$.

The above gives a natural correspondence between locally-$\mathrm{D}_4$ pairs and smooth completions of faithful amalgams of index $(4, 2)$ and of local type $\mathrm{D}_4$. Theorem 2 can now be reformulated as follows.

**Theorem 30.** *Let $(L, B, R)$ be a faithful amalgam of index $(4, 2)$ and local type $\mathrm{D}_4$. Let $m = |L|$ and let $N$ be a normal subgroup of $G^* = L *_B R$ of finite index $n$ which intersects both $L$ and $R$ trivially. Then either*

$$n \geq 2m^2 \log_2(m/2)$$

*or the corresponding coset graph $\mathrm{Cos}(G^*/N, L, a)$ is isomorphic either to $\mathrm{C}(r, s)$ for some $r \geq 3$, $1 \leq s \leq \frac{r}{2}$ or to a graph from Tables 1 and 2.*

Faithful amalgams of local type $\mathrm{D}_4$ were completely determined by Djoković [7]. One of the consequences of his work is that in a faithful amalgam $(L, B, R)$ of local type $\mathrm{D}_4$, the normaliser $N_L(B)$ of $B$ in $L$ has index $2$ in $L$ and is a nilpotent group of class at most $2$. Note that if the amalgam $(L, B, R)$ arises from the locally-$\mathrm{D}_4$ pair $(\mathrm{C}(r, s), G)$, then $N_L(B)$ is elementary abelian. This, together with Theorem 30, gives the following interesting consequence.

**Corollary 31.** *Let $(L, B, R)$ be a faithful amalgam of index $(4, 2)$ and local type $\mathrm{D}_4$ such that $N_L(B)$ is not elementary abelian. Let $|L| = m$ and let $N$ be a normal subgroup of $G^* = L *_B R$ of finite index $n$ which intersects both $L$ and $R$ trivially. Then either*

$$n \geq 2m^2 \log_2(m/2)$$

*or $\mathrm{Cos}(G^*/N, L, a)$ is one of the graphs in Tables 1 and 2.*

Finally let us mention an interesting result proved recently by Meierfrankenfeld and Sami [15], which states that if $N$ and the amalgam $(L, B, R)$ are as in Corollary 31 and $n$ is odd, then $m \leq 32$. Corollary 31 can therefore be viewed as a partial generalisation of the results in [15], where the condition on the index $n = |G^* : N|$ being odd is dropped, and the resulting upper bound on $m$ is of the form $o(\sqrt{n})$.

*Acknowledgments.* The second author is supported by UWA as part of the Australian Council Federation Fellowship Project FF0776186.

# References


[1] Barry, M. J. J.: Large Abelian Subgroups of Chevalley Groups. J. Austral. Math. Soc. Ser A **27**, 59–87 (1979).

[2] Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symbolic Comput. **24** (3-4), 235–265 (1997).

[3] Conder, M., Walker, C.: Vertex-Transitive Non-Cayley Graphs with Arbitrarily Large Vertex-Stabilizer. J. Algebraic Comb. **8**, 39–38 (1998).

[4] Conder, M., Dobcsányi, P.: Trivalent symmetric graphs on up to 768 vertices. J. Combin. Math. Combin. Comput. **40**, 41–63 (2002).

[5] Conway, J. H., Curtis, R. T., Norton, S. P., Parker, R. A., Wilson, R. A.: Atlas of Finite groups. Claredon Press, Oxford (1985).

[6] Dixon, J. D., Mortimer, B.: Permutation Groups. Springer-Verlag, New York, (1996).

[7] Djoković, D. Ž.: A class of finite group-amalgams. Proc. Amer. Math. Soc. **80**, 22–26 (1980).

[8] Gardiner, A.: Arc-Transitivity in Graphs. Quart. J. Math. Oxford Ser $(2)$ **24**, 399–407 (1973).

[9] Gardiner, A., Praeger, C. E.: On $4$-valent symmetric graphs. European J. Combin. **15**, 375–381 (1994).

[10] Gardiner, A., Praeger, C. E.: A Characterization of Certain Families of 4-Valent Symmetric Graphs. European J. Combin. **15**, 383–397 (1994).

[11] Gorenstein, D., Lyons, R., Solomon, R.: The classification of the Finite Simple Groups, Number $3$. Mathematical Surveys and Monographs Vol 40, (1998).

[12] Kleidman, P., Liebeck, M.: The Subgroup Structure of the Finite Classical Groups. London Mathematical Society, Lecture Note Series $129$, Cambridge University Press, (1990).

[13] Lawther, R.: $2F$-modules, abelian sets of roots and 2-ranks. J. Algebra **307**, 614–642 (2007).

[14] Li, C. H., Praeger, C. E., Zhou, S.: A class of finite symmetric graphs with $2$-arc-transitive quotients. Math. Proc. Cambridge Philos. Soc. **129**, 19–34 (2000).

[15] Meierfrankenfeld, U., Sami, A. Q.: Classification of finite completions of a class locally $D_8$ amalgams. Comm. Algebra **38**, 908–919 (2010).

[16] Potočnik, P., Wilson, S.: Tetravalent edge-transitive graphs of girth at most $4$. J. Combin. Theory Ser. B **97**, 217–236 (2007).

[17] Potočnik, P.: A list of 4-valent $2$-arc-transitive graphs and finite faithful amalgams of index $(4, 2)$. European J. Combin. **30**, 1323–1336 (2009).

[18] Potočnik, P., Verret, G.: On the vertex-stabiliser of arc-transitive digraphs, to appear in J. Combin. Theory, ser. B, doi:10.1016/j.jctb.2010.03.002.

[19] Potočnik, P., Spiga, P., Verret, G.: Tetravalent arc-transitive graphs with unbounded vertex-stabilisers, submitted.

[20] Praeger, C. E., Xu, M. Y.: A Characterization of a Class of Symmetric Graphs of Twice Prime Valency. European J. Combin. **10**, 91–102 (1989).

[21] Ree, R.: A family of simple groups associated with the simple Lie algebra of type $G_2$. Bull. Amer. Math. Soc. **66**, 508–510 (1960).

[22] Robinson, D. J. S.: A Course in the Theory of Groups. Springer-Verlag, New York, (1993).

[23] Serre, J. -P.: Trees. Springer-Verlag, New York, (1980).

[24] Suzuki, M.: On a class of doubly transitive groups. Ann. of Math. **75**, 105–145 (1962).

[25] Suzuki, M.: Group Theory I. Springer-Verlag, (1982).

[26] Suzuki, M.: Group Theory II. Springer-Verlag, (1986).

[27] Trofimov, V. I.: Graphs with projective suborbits. Cases of small characteristics. I (in Russian). Russian Acad. Sci. Izv. Math. **45**, 353–398 (1995).

[28] Trofimov, V. I.: Graphs with projective suborbits. Cases of small characteristics. II (in Russian). Russian Acad. Sci. Izv. Math. **45**, 559–576 (1995).

[29] Tutte, W. T.: A family of cubical graphs. Proc. Cambridge Philos. Soc **43**, 459–474 (1947).

[30] Tutte, W. T.: On the symmetry of cubic graphs. Canad. J. Math. **11**, 621–624 (1959).

[31] Vdovin, E. P.: Large Abelian Unipotent Subgroups of Finite Chevalley Groups. Algebra and Logica **40**, 292–305 (2001).

[32] Weiss, R.: An application of $p$-factorization methods to symmetric graphs. Math. Proc. Cambridge Philos. Soc. **85**, 43–48 (1979).

[33] Wilson, S.: `http://jan.ucc.nau.edu/ swilson/C4Site/BigTable.html`.

[34] Wilson, S.: Hill Capping. J. Graph Theory, accepted.

[35] Wong, W. J.: Abelian unipotent subgroups of finite orthogonal groups. J. Austral. Math. Soc. Ser. A **32**, 223–245 (1982).

[36] Wong, W. J.: Abelian unipotent subgroups of finite unitary group. J. Austral. Math. Soc. Ser. A **33**, 331–344 (1982).

[37] Xu, M. Y.: Some work on vertex-transitive graphs by Chinese mathematicians. In: Group Theory in China. Science Press Kluwer Academic Publishers, Beijing, New York (1996), 224–254.